means for distributing secure digital information to a user;

means for specifying secure control information controlling at least one condition for use of said digital information; and

means for allowing a government agency to securely, independently contribute secure control information for automatically governing tax payments for said commercial events.

219. A method of governing privacy rights related to electronic events characterized by a first step of a first party protecting digital information containing information descriptive of preventing a second party from at least one unauthorized use and a second step of specifying certain control information related to use of at least a portion of said protected digital information, wherein said control information enforces at least one right of said second party related to privacy and/or permitted use(s) of personal and/or proprietary information included in said protected digital information.

220. A system for governing privacy rights related to electronic events characterized by:

means for permitting a first party to protect digital information containing information descriptive of preventing a second party from at least one unauthorized use;

means for specifying certain control information related to use of at least a portion of said protected digital information; and

means for using the control information to enforce at least one right of said second party related to privacy and/or permitted use(s) of personal and/or proprietary information included in said protected digital information.

221. A method of governing privacy rights related to electronic events characterized by a first step of a first party protecting digital information from at least one unauthorized use and stipulating certain control information for establishing conditions for use of said protected information and a second step of a user of said digital information stipulating further control information regulating the reporting of information regarding said user's use of at least a portion of said digital information.

222. A system for governing privacy rights related to electronic events characterized by:

means for allowing a first party to protect digital information from at least one unauthorized use and for stipulating certain control information for establishing conditions for use of said protected information; and

means for allowing a user of said digital information to stipulate further control information regulating the reporting of

information regarding said user's use of at least a portion of said digital information.

223. A secure method for regulating electronic conduct and commerce characterized by a step of distributing interoperable protected processing environments and circulating amongst plural recipients of said protected processing environments software containers containing digital content and related content control information prepared for use by at least a portion of said protected processing environments, wherein said method includes the further step of regulating the use at least some of said digital content based, at least in part, on the secure processing of at least a portion of said control information through the use of at least one protected processing environment.

224. A secure system for regulating electronic conduct and commerce characterized by:

distributed interoperable protected processing environments,

means for circulating, amongst said protected processing environments, software containers containing digital content and related content control information prepared for use by at least a portion of said protected processing environments, and

means within at least some of the protected processing environments for regulating the use at least some of said digital

content based, at least in part, on the secure processing of at least a portion of said control information.

225. A method of electronic commerce networking for enabling a secure electronic retail environment characterized by the step of supplying user certified control information, smart cards, secure processing units, and retailing terminal arrangements networked together using VDE communication techniques and secure software containers.

226. An electronic commerce networking system for enabling a secure electronic retail environment characterized by:

means for networking together smart cards, secure processing units, and retailing terminal arrangements; and

means for making the smart cards, secure processing units, and retailing terminal arrangements interoperable with one another and with VDE communication techniques and secure software containers.

227. A method of enabling electronic commerce appliances for securely administering user rights in commerce activities characterized by the step of providing to users at least a portion of a VDE node contained within a physical device, said device being configured to be compatible with mating connectors in host

systems for supporting secure, interoperable transaction activity between plural parties.

228. A system for securely administering user rights in commerce activities comprising a physical device including at least a portion of a portable VDE node, said device being configured to be compatible with mating connectors in host systems for supporting secure, interoperable transaction activity between plural parties.

229. A method for enabling a programmable, electronic commerce environment characterized by the step of providing to multiple parties secure commerce nodes that securely process separate, modular component billing management methods, budgeting management methods, metering management methods, and related auditing management methods and further characterized by the step of supporting triggering of metering, auditing, billing, and budgeting methods in response to electronic commerce event activities.

230. A programmable, electronic commerce environment characterized by secure commerce nodes each including:

means for securely processing separate, modular component billing management methods, budgeting management

methods, metering management methods, and related auditing management methods, and

means for supporting triggering of metering, auditing, billing, and budgeting methods in response to electronic commerce event activities.

231. An electronic commerce system including modular, standardized control components comprising electronic commerce event control instructions stipulated by commerce participants, and plural electronic appliances containing one or more secure processing units which process at least a portion of such commerce event control instructions, said system further containing one or more databases, operatively connected to at least one of the secure processing units, for at least in part securely storing at least a portion of such control instructions for use by said at least one secure processing unit.

232. In an electronic commerce system including modular, standardized control components comprising electronic commerce event control instructions stipulated by commerce participants, and plural electronic appliances containing one or more secure processing units which process at least a portion of such commerce event control instructions, a method characterized by the step of providing one or more secure databases, operatively connected to at least one of the secure processing units, and at

least in part securely storing, within the secure databases, at least a portion of such control instructions for use by said at least one secure processing unit.

233. A content distribution system comprising plural electronic appliances containing one or more interoperable secure processing units operatively connected to one or more databases for use with at least one of said secure processing units, said one or more databases containing (a) one or more decryption keys for use in decrypting distributed, encrypted digital information, and (b) encrypted audit information, said audit information reflecting at least one aspect of use of said distributed digital information

234. A content distribution method comprising:

distributing plural electronic appliances containing one or more interoperable secure processing units

operatively connecting the appliances to one or more databases,

storing within said one or more databases one or more decryption keys,

using the decryption keys for decrypting distributed, encrypted digital information, and

storing within the one or more databases encrypted audit information, said audit information reflecting at least one aspect of use of said distributed digital information.

235. An electronic currency system comprising plural, electronic appliances containing (a) protected processing environments, (b) encrypted electronic currency and related secure control information configured so as to be useable by at least one of said protected processing environments, and (c) usage reporting means for securely communicating electronic currency usage related information from a first interoperable protected processing environment to a second interoperable protected processing environment.

236. An electronic currency method comprising:

distributing plural, electronic appliances containing (a) protected processing environments, (b) encrypted electronic currency and related secure control information configured so as to be useable by at least one of said protected processing environments, and

securely communicating electronic currency usage related information from a first interoperable protected processing environment to a second interoperable protected processing environment.

237. A method for electronic financial activities characterized by the steps of:

communicating digital containers containing financial information from a first interoperable secure node to a second interoperable secure node,

communicating modular, standard control information to said second secure node to, at least in part, set the conditions for use of at least a portion of said financial information,

reporting information related to said use to said first interoperable secure node.

238. A system for electronic financial activities characterized by:

means for communicating digital containers containing financial information from a first interoperable secure node to a second interoperable secure node,

means for communicating modular, standard control information to said second secure node,

means at the second node for, at least in part, setting the conditions for use of at least a portion of said financial information, and

means for reporting information related to said use from the second secure node to said first interoperable secure node.

239. A method for electronic currency management including:

communicating encrypted electronic currency from a first, interoperable secure user node to a second interoperable user node using at least one secure container, and

providing secure control information for use with said at least one secure container, said secure control information, at least in part, maintaining conditionally anonymous currency usage information.

240. A system for electronic currency management including:

means for communicating encrypted electronic currency from a first, interoperable secure user node to a second interoperable user node using at least one secure container, and

means for providing secure control information for use with said at least one secure container, said secure control information, at least in part, maintaining conditionally anonymous currency usage information.

241. A method for electronic financial activities management characterized by the steps of:

securely communicating from a first secure node to a second secure node financial information standardized control information for controlling the use of financial information used in a financial value chain,

securely communicating from said first secure node to a third secure node said financial information standardized control information for controlling the use of financial information used in a financial value chain,

securely communicating encrypted financial information from said second secure node to said third secure node, including communicating secure control information,

processing said financial information at said third node at least in part through the use of secure control information supplied by said first and said second secure nodes, wherein said standardized control information is at least in part stored in a secure database contained within said third secure node.

242. A system for electronic financial activities management characterized by the steps of:

means coupled to a first and a second secure node for securely communicating from said first secure node to said second secure node financial information standardized control information for controlling the use of financial information used in a financial value chain,

means coupled between the first secure node and a third secure node for securely communicating from said first secure node to said third secure node said financial information standardized control information for controlling the use of financial information used in a financial value chain,

means coupled between the second and third nodes for securely communicating encrypted financial information from said second secure node to said third secure node, including communicating secure control information, and

means at the third node for processing said financial information at said third node at least in part through the use of secure control information supplied by said first and said second secure nodes, and

a secure database at the third node for at least in part storing said standardized control information.

243. A method of information management characterized by the steps of creating at least one smart object at a first location, protecting at least a portion of said smart object including protecting at least one rule and/or control assigned to said smart object, distributing said at least one smart object to at least one second location, securely processing at least a portion of the contents of said at least one smart object at said at least one second location in accordance with at least a portion of at least one said rule and/or control assigned to said smart object.

244. An information management system characterized by:

means for creating at least one smart object at a first location,

means for protecting at least a portion of said smart object including means for protecting at least one rule and/or control assigned to said smart object,

means for distributing said at least one smart object to at least one second location, and

means for securely processing at least a portion of the contents of said at least one smart object at said at least one second location in accordance with at least a portion of at least one said rule and/or control assigned to said smart object.

245. An object processing system comprising at least one secure object containing at least in part protected executable content and at least one at least in part protected rule and/or control associated with operations related to the execution of such content, and at least one secure execution environment for processing the executable content in accordance with at least a portion of at least one of said at least one associated rule and/or control.

246. An object processing method comprising:

providing at least one secure object containing at least in part protected executable content and at least one at least in part protected rule and/or control associated with operations related to the execution of such content,

processing, within at least one secure execution environment, the executable content in accordance with at least a portion of at least one of said at least one associated rule and/or control.

247. A rights distributed database environment including (a) means allowing one or more central authorities to establish control information for use of encrypted digital information, (b) interoperable database management systems at plural user sites for securely storing control information and audit information, (c) secure communication means for securely communicating control information and audit information between user sites, and (d) centralized database means for compiling and analyzing usage information from plural user sites.

248. Within a rights distributed database environment, a method characterized by the following steps:

establishing control information for use of encrypted digital information,

securely storing, within interoperable database management systems at plural user sites, control information and audit information,

securely communicating control information and audit information between user sites, and

compiling and analyzing usage information from plural user sites.

249. A method of distributed database searching characterized by the steps of creating at least one secure object containing search criteria, transmitting at least one such secure object to one or more second locations to perform database searches in accordance with at least one rule and/or control, processing at least one database search based at least in part on the search criteria within a secure object in accordance with at least a portion of at least one of the said at least one associated rule and/or control, storing database search results in the same and/or one or more new secure objects, and transmitting the secure object containing search results to the first location.

250. A method as in claim 247 further characterized by the additional step of associating at least one additional rule and/or control with the search results for establishing at least one condition related to the use of at least one portion of said search results.

251. A system for distributed database searching characterized by:

means for creating at least one secure object containing search criteria,

means for transmitting at least one such secure object to one or more second locations to perform database searches in accordance with at least one rule and/or control,

means for processing at least one database search based at least in part on the search criteria within a secure object in accordance with at least a portion of at least one of the said at least one associated rule and/or control,

means for storing database search results in the same and/or one or more new secure objects, and

means for transmitting the secure object containing search results to the first location.

252. A system as in claim 249 further characterized by means for associating at least one additional rule and/or control with the search results for establishing at least one condition related to the use of at least one portion of said search results.

253. A rights management system comprising protected information, at least two protected processing arrangements, and a rights management language that allows the expression of permitted operations and the consequences of performing such operations on at least a portion of the information processed at least in part by at least one of the protected processing arrangements.

254. A rights management method comprising:

providing protected information for processing by at least two protected processing arrangements, and

expressing, in a rights management language, permitted operations and the consequences of performing such operations on at least a portion of the information processed at least in part by at least one of the protected processing arrangements.

255. A method of protecting digital information characterized by the steps of encrypting at least a portion of the information, using a rights management language to describe the conditions related to use of the information, distributing at least a portion of such information and at least a portion of such rights language expressed conditions to one or more recipients, using an electronic appliance arrangement including at least one protected processing arrangement to securely govern at least a portion of the use of such information.

256. A system for protecting digital information characterized by:

means for encrypting at least a portion of the information,

means for using a rights management language to describe the conditions related to use of the information,

means for distributing at least a portion of such information and at least a portion of such rights language expressed conditions to one or more recipients, and

an electronic appliance arrangement including at least one protected processing arrangement for securely governing at least a portion of the use of such information.

257. A distributed digital information management system comprising software components, a rights management language for expressing processing relationships between two or more of the software components, protected processing means for at least a portion of the software components and at least a portion of the rights management expressions, means for protecting content, means for creating software objects that relate protected content to rights management expressions, and means for delivering protected content, rights management expressions, and such software objects from a providing location to a user's location.

258. A distributed digital information management method comprising:

expressing, in a rights management language, processing relationships between two or more of the software components,

processing, within at least one protected environment, at least a portion of the software components and at least a portion of the rights management expressions,

protecting content,

creating software objects that relate protected content to rights management expressions, and

delivering protected content, rights management expressions, and such software objects from a providing location to a user's location.

259. An authentication system comprising at least two electronic appliances, at least two digital certificates reflecting identity information encrypted using different certifying private keys where such certificates are stored in a first electronic appliance, communications means for transmitting and receiving signals between electronic appliances, means for determining compromised and/or expired certifying private keys operatively connected to a second electronic appliance, means for the second electronic appliance to request transmission of one of the digital certificates from the first electronic appliance based at least in part on such determination, and means operatively connected to such second electronic appliance for decrypting such certificate and determining such certificate's validity and/or the validity of identity information.

260. In a system comprising at least two electronic appliances, an authenticating method comprising:

issuing at least two digital certificates reflecting identification information, including the step of encrypting the two certificates using different certifying private keys,

storing the certificates in a first electronic appliance,

transmitting and receiving signals between electronic appliances,

determining compromised and/or expired certifying private keys operatively connected to a second electronic appliance,

requesting, with the second electronic appliance, transmission of one of the digital certificates from the first electronic appliance based at least in part on such determination,

decrypting such certificate with the second electronic appliance, and

determining such certificate's validity and/or the validity of identity information.

261. An authentication system comprising at least two electronic appliances, at least two digital certificates reflecting identify information encrypted using different certifying private keys where such certificates are stored in a first electronic appliance, communications means for transmitting and receiving signals between electronic appliances, means for a second electronic appliance to request transmission of one of the digital certificates from the first electronic appliance wherein the selection of which certificate is requested is based at least in part

on a random or pseudo-random number, means operatively connected to such second electronic appliance for decrypting such certificate and determining such certificate's validity and/or the validity of identity information.

262. In a system comprising at least two electronic appliances, an authenticating method comprising:

issuing at least two digital certificates reflecting identify information, including the step of encrypting the two digital certificates using different certifying private keys,

storing such certificates in a first electronic appliance,

transmitting and receiving signals between electronic appliances,

requesting, with a second electronic appliance, transmission of one of the digital certificates from the first electronic appliance, including the step of selecting a certificate based at least in part on a random or pseudo-random number,

decrypting such certificate with the second electronic appliance; and

determining such certificate's validity and/or the validity of identity information.

263. A method of secure electronic mail characterized by the steps of creating at least one electronic message using an interoperable protected processing environment, encrypting at

least a portion of said at least one message, securely associating one or more sets of control information with one or more messages to set at least one condition for the use of said at least one message, communicating the protected electronic messages to one or more recipients having protected processing environments, securely communicating at least one set of the same or differing control information to each recipient, enabling recipients of both control information and protected messages to use message information at least in part in accordance with the conditions specified by the control information.

264. A system for secure electronic mail including multiple protected processing environments, the system characterized by:

a first protected processing environment for creating at least one electronic message, the first environment including means for encrypting at least a portion of said at least one message, means for securely associating one or more sets of control information with one or more messages to set at least one condition for the use of said at least one message, and means for communicating the protected electronic messages to one or more recipients having interoperable protected processing environments,

means for securely communicating at least one set of the same or differing control information to each recipient, and

means for enabling recipients of both control information and protected messages to use message information at least in part in accordance with the conditions specified by the control information.

265. A method of information management characterized by the steps of protecting content from unauthorized use, securely associating enabling control information with at least a portion of such protected content wherein such enabling control information incorporates information describing how the enabling control information may be redistributed, delivering at least a portion of the protected content to a first user, delivering such enabling control information to such first user, receiving a request to redistribute such enabling control information from such first user, using the description of how enabling control information may be redistributed to create new enabling control information where such new enabling control information may be the same or different than the enabling control information received by such first user, delivering the new enabling control information and/or protected information to a second user.

266. An information management system characterized by:

means for protecting content from unauthorized use,

means for securely associating enabling control information with at least a portion of such protected content, including means for incorporating enabling control information describing how the enabling control information may be redistributed,

means for delivering at least a portion of the protected content to a first user,

means for delivering such enabling control information to such first user,

means for receiving a request to redistribute such enabling control information from such first user,

means for using the description of how enabling control information may be redistributed to create new enabling control information where such new enabling control information may be the same or different than the enabling control information received by such first user, and

means for delivering the new enabling control information and/or protected information to a second user.

267. A method of controlling redistribution of distributed digital information including the steps of encrypting digital information, distributing said encrypted digital information from a first party to a second party, establishing control information regarding the redistribution of at least a portion of said encrypted digital information from said second party to at least one third

party, regulating the redistribution of said at least a portion of said encrypted digital information through the use of a protected processing environment processing said control information.

268. A system for controlling redistribution of distributed digital information including:

means for encrypting digital information,

means for distributing said encrypted digital information from a first party to at least one second party,

means for establishing control information regarding the redistribution of at least a portion of said encrypted digital information from said second party to at least one third party, and

a protected processing environment for processing said control information and for regulating the redistribution of said at least a portion of said encrypted digital information.

269. A method of controlling a robot characterized by the steps of creating instructions for one or more robots, creating a secure container incorporating such instructions, associating control information with such secure container, incorporating at least one secure processing unit into such one or more robots, and performing at least a portion of such instructions in accordance with at least a portion of such control information.

270. A method as in claim 267 further characterized in that such control information includes information describing the conditions under which such instructions may be used and the nature of audit reports required when such instructions are performed.

271. A robot control system characterized by:

means for creating instructions for one or more robots,

means for creating a secure container incorporating such instructions,

means for associating control information with such secure container,

means for incorporating at least one secure processing unit into such one or more robots, and

means for performing at least a portion of such instructions in accordance with at least a portion of such control information.

272. A system as in claim 269 further characterized by means for creating such control information, including means for describing the conditions under which such instructions may be used and the nature of audit reports required when such instructions are performed.

273. A method of detecting fraud in electronic commerce characterized by the steps of creating at least one secure

container, associating control information with such one or more containers including control information requiring that audit information be collected and transmitted to an auditing party, delivering such one or more containers and such control information to at least one user, recording information identifying each container and each such user, receiving audit information, creating a profile of usage based at least in part on such received audit information and/or such control information, detecting cases where certain audit information differs at least in part from such profile of usage.

274. A system for detecting fraud in electronic commerce characterized by

means for creating at least one secure container,

means for associating control information with such one or more containers including control information requiring that audit information be collected and transmitted to an auditing party,

means for delivering such one or more containers and such control information to at least one user,

means for recording information identifying each container and each such user,

means for receiving audit information,

means for creating a profile of usage based at least in part on such received audit information and/or such control information, and

means for detecting cases where certain audit information differs at least in part from such profile of usage.

275. A method of detecting fraud in electronic commerce characterized by the steps of distributing at least in part protected digital information to customers, distributing one or more rights to use at least a portion of such digital information across an electronic network, allowing a customer to use at least a part of said at least in part protected digital information through the use of a protected processing environment and at least one of said one or more distributed rights, detecting unusual usage activity related to use of said digital information.

276. A system for detecting fraud in electronic commerce characterized by

means for distributing at least in part protected digital information to customers,

means for distributing one or more rights to use at least a portion of such digital information across an electronic network,

a protected processing environment for allowing a customer to use at least a part of said at least in part protected

digital information through at least one of said one or more distributed rights, and

means for detecting unusual usage activity related to use of said digital information.

277. A programmable component arrangement comprising a tamper resistant processing environment including a microprocessor, memory, a task manager, memory manager and external interface controller, means for loading arbitrary components at least in part into the memory, means for initiating one or more tasks associated with processing such components, means for certifying the validity, integrity and/or trustedness of such components, means for creating arbitrary components, means for associating arbitrary events with such created components, means for certifying the validity, integrity and/or trustedness of such created components, and means for securely delivering such created components.

278. In a programmable component arrangement comprising a tamper resistant processing environment including a microprocessor, memory, a task manager, memory manager and an external interface controller, a processing method characterized by the following steps:

creating arbitrary components,

associating arbitrary events with such created components,

loading the arbitrary components at least in part into the memory,

initiating one or more tasks associated with processing such loaded components,

certifying the validity, integrity and/or trustedness of such created components, and

securely delivering such created components.

279. A distributed, protected, programmable component arrangement comprising at least two tamper resistant processing environments including a microprocessor, memory, a task manager, memory manager and external interface controller, means for loading arbitrary components at least in part into the memory, means for initiating one or more tasks associated with processing such components, and means for certifying the validity, integrity and/or trustedness of such components, said arrangement further comprising means for creating arbitrary components, means for associating arbitrary events with such created components, means for certifying the validity, integrity and/or trustedness of such created components, means for securely delivering such created components between at least two of said at least two tamper resistant processing environments.

280. In a distributed, protected, programmable component arrangement comprising at least two tamper resistant processing

environments including a microprocessor, memory, a task manager, memory manager and external interface controller, a method comprising

creating arbitrary components,

certifying the validity, integrity and/or trustedness of such components,

loading arbitrary components at least in part into the memory,

initiating one or more tasks associated with processing such components,

associating arbitrary events with such created components, and

securely delivering such created components between at least two of said at least two tamper resistant processing environments.

281. An electronic appliance comprising at least one CPU, memory, at least one system bus, at least one protected processing environment, and at least one of a Rights Operating System or Rights Operating System layer associated with a host operating system.

282. An operating system comprising at least one task manager, at least one memory manager, at least one input/output manager, at least one protected processing environment, means

for detecting events, means for associating events with rights control functions, means for performing rights control functions at least in part within such one or more protected processing environments.

283. In an operating system comprising at least one task manager, at least one memory manager, at least one input/output manager, at least one protected processing environment, an operating method comprising:

detecting events,

associating events with rights control functions, and

performing rights control functions at least in part within such one or more protected processing environments.

284. A method of business automation characterized by the steps of creating one or more secure containers including accounting and/or other administrative information, associating control information with such one or more secure containers including a description of (a) the one or more parties to whom the container may and/or must be delivered and/or (b) the operations that one or more parties may and/or must perform with respect to such accounting and/or other administrative information, delivering one or more of such containers to one or more parties, and enabling the description and/or enforcement of at least a portion of such control information prior, during and/or

subsequent to use of such accounting and/or other administrative information by one or more parties.

285. A method as in claim 282 where such control information further includes at least one requirement that audit information be collected and delivered to one or more auditing parties, and further includes the step of delivering at least a portion of such audit information to one or more parties.

286. A method as in claim 283 where at least a portion of such audit information is automatically processed by at least one of such auditing parties, and further includes the step of transmitting further accounting, administrative and/or audit information to one or more parties that may be the same and/or differ from the one or more parties from whom audit information was received based at least in part on the receipt and/or content of such received audit information.

287. A method as in claim 282 where at least two of such parties are associated with different businesses and/or other organizations and such control information includes information that at least in part describes an accounting, administrative, reporting and/or other audit relationship between such businesses and/or other organizations.

288. A method as in claim 282, 283, 284, or 285 where some or all of such accounting and/or other administrative information is included in such control information.

289. A business automation system characterized by:

means for creating one or more secure containers including accounting and/or other administrative information,

means for associating, with such one or more secure containers, control information including a description of (a) the one or more parties to whom the container may and/or must be delivered and/or (b) the operations that one or more parties may and/or must perform with respect to such accounting and/or other administrative information,

means for delivering one or more of such containers to one or more parties, and

means for enabling the description and/or enforcement of at least a portion of such control information prior, during and/or subsequent to use of such accounting and/or other administrative information by one or more parties.

290. A system as in claim 287 where the associating means further includes means for associating at least one requirement that audit information be collected and delivered to one or more auditing parties, and the delivering means includes

means for delivering at least a portion of such audit information to one or more parties.

291. A system as in claim 288 further including means for automatically processing at least a portion of such audit information, and the system further includes means for transmitting further accounting, administrative and/or audit information to one or more parties that may be the same and/or differ from the one or more parties from whom audit information was received based at least in part on the receipt and/or content of such received audit information.

292. A system as in claim 287 where at least two of such parties are associated with different businesses and/or other organizations and the associating means includes means for generating control information including information that at least in part describes an accounting, administrative, reporting and/or other audit relationship between such businesses and/or other organizations.

293. A system as in claim 286, 287, 288, or 290 where some or all of such accounting and/or other administrative information is included in such control information.

294. A method of distributing content characterized by the steps of creating one or more first secure containers, associating control information with such first containers including information describing the conditions under which some or all of the content of such first containers may be extracted, delivering at least a portion of such first containers and such control information to one or more parties, detecting a request by one or more of such parties to extract some or all of the content of such first containers, determining if such request is permitted in whole or in part by such control information, to the extent permitted by such control information creating one or more second secure containers in accordance with such request and such control information, associating control information with such one or more second secure containers based at least in part on control information associated with such first containers.

295. A system for distributing content characterized by:

means for creating one or more first secure containers,

means for associating control information with such first containers including information describing the conditions under which some or all of the content of such first containers may be extracted,

means for delivering at least a portion of such first containers and such control information to one or more parties,

means for detecting a request by one or more of such parties to extract some or all of the content of such first containers,

means for determining if such request is permitted in whole or in part by such control information, to the extent permitted by such control information creating one or more second secure containers in accordance with such request and such control information, and

means for associating control information with such one or more second secure containers based at least in part on control information associated with such first containers.

296. A method of distributing content characterized by the steps of creating one or more first secure containers, associating control information with such first secure containers including information describing the conditions under which such first secure containers (a) may in whole or in part be embedded into and/or securely associated with one or more second secure containers and/or (b) may allow one or more secure containers to be in whole or in part embedded into and/or securely associated with such first secure containers, delivering at least a portion of such first secure containers and such control information to one or more parties, detecting a request by one or more of such parties or by additional parties to (a) in whole or in part embed into and/or securely associate with such first containers one or

more second containers and/or (b) in whole or in part embed into and/or securely associate with a secure container such first secure containers, determining if such request is permitted by control information, to the extent permitted by control information performing one or more embedding and/or secure association operations, to the extent required by control information and/or requested by one or more of such parties, modifying and/or creating new control information at least in part as a consequence of such one or more embedding and/or secure association operations.

297. A system for distributing content characterized by

means for creating one or more first secure containers,

means for associating control information with such first secure containers including information describing the conditions under which such first secure containers (a) may in whole or in part be embedded into and/or securely associated with one or more second secure containers and/or (b) may allow one or more secure containers to be in whole or in part embedded into and/or securely associated with such first secure containers,

means for delivering at least a portion of such first secure containers and such control information to one or more parties,

means for detecting a request by one or more of such parties to (a) in whole or in part embed into and/or securely associate with such first containers one or more second

containers and/or (b) in whole or in part embed into and/or securely associate with a secure container such first secure containers, and

means for determining if such request is permitted by control information, to the extent permitted by control information performing one or more embedding and/or secure association operations, to the extent required by control information and/or requested by one or more of such parties, modifying and/or creating new control information at least in part as a consequence of such one or more embedding and/or secure association operations.

298. A method of distributing information characterized by the steps of protecting information from unauthorized use, associating control information with such protected information, delivering at least a portion of such protected information to one or more parties using plural pathways, delivering at least a portion of such control information to one or more parties using the same or different plural pathways, enabling at least one of such parties to make at least some use of such protected information delivered using a first pathway in accordance with control information at least a portion of which is delivered using a second pathway.

299. A method as in claim 296 in which at least one of such pathways of delivering protected information and/or control information is described by such control information.

300. A system for distributing information characterized by:

means for protecting information from unauthorized use,

means for associating control information with such protected information,

means for delivering at least a portion of such protected information to one or more parties using plural pathways,

means for delivering at least a portion of such control information to one or more parties using the same or different plural pathways,

means for enabling at least one of such parties to make at least some use of such protected information delivered using a first pathway in accordance with control information at least a portion of which is delivered using a second pathway.

301. A system as in claim 298 wherein the delivering means includes means for delivering, over at least one of such pathways, protected information and/or control information described by such control information.

302. A method of distributing information characterized by the steps of protecting information from unauthorized use, associating control information with such protected information including information requiring the collection of audit information, enabling one or more parties to receive and/or process audit information, delivering at least a portion of such protected information and such control information to one or more parties, enabling at least some use of such protected information in accordance with at least a portion of such control information that requires the collection of audit information, delivering such audit information to one or more of such enabled auditing parties different from such delivering party or parties.

303. A method as in claim 300 in which at least one of such auditing parties is specified in such control information.

304. A system for distributing information characterized by

means for protecting information from unauthorized use,

means for associating control information with such protected information including information requiring the collection of audit information,

means for enabling one or more parties to receive and/or process audit information,

means for delivering at least a portion of such protected information and such control information to one or more parties,

means for enabling at least some use of such protected information in accordance with at least a portion of such control information that requires the collection of audit information, and

means for delivering such audit information to one or more of such enabled auditing parties different from such delivering party or parties.

305. A system as in claim 302 in which at least one of such auditing parties is specified in such control information.

306. A secure component-based operating process including:

(a) retrieving at least one component;

(b) retrieving a record that specifies a component assembly;

(c) checking said component and/or said record for validity;

(d) using said component to form said component assembly in accordance with said record; and

(e) performing a process based at least in part on said component assembly.

307. A process as in claim 304 wherein said step (c) further comprises executing said component assembly.

308. A process as in claim 304 wherein said component comprises executable code.

309. A process as in claim 304 wherein said component comprises a load module.

310. A process as in claim 304 wherein:

said record comprises:

(i) directions for assembling said component assembly; and

(ii) information that at least in part specifies a control; and

said process further comprises controlling said step (d) and/or said step (e) based at least in part on said control.

311. A process as in claim 304 wherein said component has a security wrapper, and said controlling step comprises selectively opening said security wrapper based at least in part on said control.

312. A process as in claim 304 wherein:

said permissions record includes at least one decryption key; and

said controlling step includes controlling use of said decryption key.

313. A process as in claim 304 including performing at least two of said steps (a) and (e) within a protected processing environment.

314. A process as in claim 304 including performing at least two of said steps (a) and (e) at least in part within tamper-resistant hardware.

315. A method as in claim 304 wherein said performing step (e) includes metering usage.

316. A method as in claim 304 wherein said performing step (e) includes auditing usage.

317. A method as in claim 304 wherein said performing step (e) includes budgeting usage.

318. A secure component operating system process including:

receiving a component;

receiving directions specifying use of said component to form a component assembly;

authenticating said received component and/or said directions;

forming, using said component, said component assembly based at least in part on said received directions; and

using said component assembly to perform at least one operation.

319. A method comprising performing the following steps within a secure operating system environment:

providing code;

providing directions specifying assembly of said code into an executable program;

checking said received code and/or said assembly directors for validity; and

in response to occurrence of an event, assembling said code in accordance with said received assembly directions to form an assembly for execution.

320. A method for managing at least one resource with a secure operating environment, said method comprising:

securely receiving a first control from a first entity external to said operating environment;

securely receiving a second control from a second entity external to said operating environment, said second entity being different from said first entity;

securely processing, using at least one resource, a data item associated with said first and second controls; and

securely applying said first and second controls to manage said resource for use with said data item.

321. A method for securely managing at least one operation on a data item performed at least in part by an electronic arrangement, said method comprising:

(a) securely delivering a first procedure to said electronic arrangement;

(b) securely delivering, to said electronic arrangement, a second procedure separable or separate from said first procedure;

(c) performing at least one operation on said data item, including using said first and second procedures in combination to at least in part securely manage said operation; and

(d) securely conditioning at least one aspect of use of said data item based on said delivering steps (a) and (b) having occurred.

322. A method as in claim 319 including performing said delivering step (b) at a time different from the time said delivering step (a) is performed.

323. A method as in claim 319 wherein said step (a) includes delivering said first procedure from a first source, and said step (b) includes delivering said second procedure from a second source different from said first source.

324. A method as in claim 319 further including ensuring the integrity of said first and second procedures.

325. A method as in claim 319 further including validating each of said first and second procedures.

326. A method as in claim 319 further including authenticating each of said first and second procedures.

327. A method as in claim 319 wherein said using step (c) includes executing at least one of said first and second procedures within a tamper-resistant environment.

328. A method as in claim 319 wherein said step (c) includes the step of controlling said data item with at least one of said first and second procedures.

329. A method as in claim 319 further including establishing a relationship between at least one of said first and second procedures and said data item.

330. A method as in claim 319 further including establishing correspondence between said data item and at least one of said first and second procedures.

331. A method as in claim 319 wherein said delivering step (b) comprises delivering at least one load module encrypted at least in part.

332. A method as in claim 329 wherein said delivering step (a) comprises delivering at least one further load module encrypted at least in part.

333. A method as in claim 319 wherein said delivering step (b) comprises delivering at least one content container carrying at least in part secure control information.

334. A method as in claim 319 wherein said delivering step (b) comprises delivering a control method and at least one further method.

335. A method as in claim 319 wherein said delivering step (a) includes:

encrypting at least a portion of said first procedure,

communicating said at least in part encrypted first procedure to said electronic arrangement,

decrypting at least a portion of said first procedure at least in part using said electronic arrangement, and

validating said first procedure with said electronic arrangement.

336. A method as in claim 319 wherein said delivering step (b) includes delivering at least one of said first and second procedures within an administrative object.

337. A method as in claim 319 wherein said delivering step (b) includes codelivering said second procedure in at least in part encrypted form with said data item.

338. A method as in claim 319 wherein said performing step includes metering usage.

339. A method as in claim 319 wherein said performing step includes auditing usage.

340. A method as in claim 319 wherein said performing step includes budgeting usage.

341. A method for securely managing at least one operation performed at least in part by a secure electronic appliance, comprising:

(a) selecting an item that is protected with respect to at least one operation;

(b) securely independently delivering plural separate procedures to said electronic appliance;

(c) using said plural separate procedures in combination to at least in part securely manage said operation with respect to said selected item; and

(d) conditioning successful completion of said operation on said delivering step (b) having occurred.

342. A method for processing based on deliverables comprising:

securely delivering a first piece of code defining a first part of a process;

separately, securely delivering a second piece of code defining a second part of said process;

ensuring the integrity of the first and second delivered pieces of code; and

performing said process based at least in part on said first and second delivered code pieces.

343. A method as in claim 340 wherein a first piece of code for said process at least in part controls decrypting content.

344. A method as in claim 340 wherein said ensuring step includes validating said first and second pieces of code.

345. A method as in claim 340 wherein said ensuring step includes validating said first and second pieces of code relative to one another.

346. A method as in claim 340 wherein said performing step includes metering usage.

347. A method as in claim 340 wherein said performing step includes auditing activities.

348. A method as in claim 340 wherein said performing step includes budgeting usage.

349. A method as in claim 340 wherein said performing step includes electronically processing content based on electronic controls.

350. A method of securely controlling at least one protected operation with respect to a data item comprising:

(a) supplying at least a first control from a first party;

(b) supplying at least a second control from a second party different from said first party;

(c) securely combining said first and second controls to form a set of controls;

(d) securely associating said control set with said data item; and

(e) securely controlling at least one protected operation with respect to said data item based on said control set.

351. A method as in claim 348 wherein said data item is protected.

352. A method as in claim 348 wherein at least one of said plural controls includes a control relating to metering at least one aspect of use of said protected data item.

353. A method as in claim 348 wherein at least one of said plural controls include a control relating to budgeting at least one aspect of use of said protected data item.

354. A secure method for combining data items into a composite data item comprising:

(a) securely providing a first data item having at least a first control associated therewith;

(b) securely providing a second data item having at least a second control associated therewith;

(c) forming a composite of said first and second data items;

(d) securely combining said first and second controls into a composite control set; and

(e) performing at least one operation on said composite of said first and second data items based at least in part on said composite control set.

355. A method as in claim 352 wherein said combining step includes preserving each of said first and second controls in said composite set.

356. A method as in claim 352 wherein said performing step comprises governing the operation on said composite of said first and second data items in accordance with said first control and said second control .

357. A method as in claim 352 wherein said providing step includes ensuring the integrity of said association between said first controls and said first data item is maintained during at least one of transmission, storage and processing of said first data item.

358. A method as in claim 352 wherein said providing step comprises delivering said first data item separately from said first control .

359. A method as in claim 352 wherein said providing step comprises codelivering said first data item and said first control .

360. A secure method for controlling a protected operation comprising:

(a) delivering at least a first control and a second control; and

(b) controlling at least one protected operation based at least in part on a combination of said first and second controls, including at least one of the following steps:

resolving at least one conflict between said first and second controls based on a predefined order;

providing an interaction with a user to form said combination; and

dynamically negotiating between said first and second controls.

361. A method as in claim 358 wherein said controlling step (b) includes controlling decryption of electronic content.

362. A method as in claim 358 further including:

receiving protected electronic content from a party; and

authenticating the identity of said party prior to using said received protected electronic content.

363. A secure method comprising:

selecting protected data;

extracting said protected data from an object;

identifying at least one control to manage at least one aspect of use of said extracted data;

placing said extracted data into a further object; and

associating said at least one control with said further object.

364. A method as in claim 361 further including limiting at least one aspect of use of said further object based on said at least one control.

365. A secure method of modifying a protected object comprising:

(a) providing a protected object; and

(b) embedding at least one additional element into said protected object without unprotecting said object.

366. A method as in claim 60 further including:

associating at least one control with said object; and

limiting usage of said element in accordance with said control.

367. A method as in claim 363 further including a permissions record within said object.

368. A method as in claim 364 further including at least in part encrypting said object.

369. A method for managing at least one resource with a secure operating environment, said method comprising:

securely receiving a first load module from a first entity external to said operating environment;

securely receiving a second load module from a second entity external to said operating environment, said second entity being different from said first entity;

securely processing, using at least one resource, a data item associated with said first and second load modules; and

securely applying said first and second load modules to manage said resource for use with said data item.

370. A method for negotiating electronic contracts, comprising:

receiving a first control set from a remote site;

providing a second control set;

performing, within a protected processing environment, an electronic negotiation between said first control set and said

second control set, including providing interaction between said first and second control sets; and

producing a negotiated control set resulting from said interaction between said first and second control sets.

371. A system for supporting electronic commerce including:

means for creating a first secure control set at a first location;

means for creating a second secure control set at a second location;

means for securely communicating said first secure control set from said first location to said second location; and

means at said second location for securely integrating said first and second control sets to produce at least a third control set comprising plural elements together comprising an electronic value chain extended agreement.

372. A system for supporting electronic commerce including:

means for creating a first secure control set at a first location;

means for creating a second secure control set at a second location;

means for securely communicating said first secure control set from said first location to said second location; and

negotiation means at said second location for negotiating an electronic contract through secure execution of at least a portion of said first and second secure control sets.

373. A system as in claim 370 further including means for controlling use by a user of protected information content based on at least a portion of said first and/or second control sets.

374. A system as in claim 370 further including means for charging for at least a part of said content use.

375. A secure component-based operating system including:

component retrieving means for retrieving at least one component;

record retrieving means for retrieving a record that specifies a component assembly;

checking means, operatively coupled to said component retrieving means and said record retrieving means, for checking said component and/or said record for validity;

using means, coupled to said checking means, for using said component to form said component assembly in accordance with said record; and

performing means, coupled to said using means, for performing a process based at least in part on said component assembly.

376. A secure component-based operating system including:

a database manager that retrieves, from a secure database, at least one component and at least one record that specifies a component assembly;

an authenticating manager that checks said component and/or said record for validity;

a channel manager that uses said component to form said component assembly in accordance with said record; and

an execution manager that performs a process based at least in part on said component assembly.

377. A secure component operating system including:

means for receiving a component;

means for receiving directions specifying use of said component to form a component assembly;

means, coupled to said receiving means, for authenticating said received component and/or said directions;

means, coupled to said authenticating means, for forming, using said component, said component assembly based at least in part on said received directions; and

means, coupled to said forming means, for using said component assembly to perform at least one operation.

378. A secure component operating environment including:

a storage device that stores a component and directions specifying use of said component to form a component assembly;

an authenticating manager that authenticates said component and/or said directions;

a channel manager that forms, using said component, said component assembly based at least in part on said directions; and

a channel that executes said component assembly to perform at least one operation.

379. A secure operating system environment comprising:

a storage device that stores code and directions specifying assembly of said code into an executable program;

a validating device that checks said received code and/or said assembly directors for validity; and

an event-driven channel that, in response to occurrence of an event, assembles said code in accordance with said assembly directions to form an assembly for execution.

380. A secure operating environment system for managing at least one resource comprising:

a communications arrangement that securely receives a first control from a first entity external to said operating environment, and securely receives a second control from a second entity external to said operating environment, said second entity being different from said first entity; and

a protected processing environment, coupled to said communications arrangement, that:

(a) securely processes, using at least one resource, a data item associated with said first and second controls, and

(b) securely applies said first and second controls to manage said resource for use of said data item.

381. A system for negotiating electronic contracts, comprising:

a storage arrangement that stores a first control set received from a remote site, and stores a second control set;

a protected processing environment, coupled to said storage arrangement, that:

(a) performs an electronic negotiation between said first control set and said second control set,

(b) provides interaction between said first and second control sets, and

(c) produces a negotiated control set resulting from said interaction between said first and second control sets.

382. A system as in claim 379 further including means for electronically enforcing said negotiated control set.

383. A system as in claim 379 further including means for generating an electronic contract based on said negotiated control set.

384. A method for supporting electronic commerce including:

creating a first secure control set at a first location;

creating a second secure control set;

electronically negotiating, at said location different from said first location, an electronic contract, including the step of securely executing at least a portion of said first and second control sets.

385. An electronic appliance comprising:

a processor; and

at least one memory device connected to said processor;

wherein said processor includes:

retrieving means for retrieving at least one component, and at least one record that specifies a component assembly, from said memory device,

checking means coupled to said retrieving means for checking said component and/or said record for validity, and

using means coupled to said retrieving means for using said component to form said component assembly in accordance with said record.

386. An electronic appliance comprising:

at least one processor;

at least one memory device connected to said processor; and

at least one input/output connection operatively coupled to said processor,

wherein said processor at least in part executes a rights operating system to provide a secure operating environment within said electronic appliance.

387. An electronic appliance as in claim 384 wherein said processor includes means for providing a channel, said channel assembling independently deliverable components into a component assembly and executing said component assembly.

388. An electronic appliance as in claim 384 further including a secondary storage device coupled to said processor, said secondary storage device storing a secure database, said processor including means for decrypting information obtained from said secure database and for encrypting information to be written to said secure database.

389. An electronic appliance as in claim 384 wherein said processor and said memory device are disposed in a secure, tamper-resistance encapsulation.

390. An electronic appliance as in claim 384 wherein said processor includes a hardware encryptor/decryptor.

391. An electronic appliance as in claim 384 wherein said processor includes a real time clock.

392. An electronic appliance as in claim 384 wherein said processor includes a random number generator.

393. An electronic appliance as in claim 384 wherein said memory device stores audit information.

394. A method for auditing the use of at least one resource with a secure operating environment, said method comprising:

securely receiving a first control from a first entity external to said operating environment;

securely receiving a second control from a second entity external to said operating environment, said second entity being different from said first entity;

using at least one resource;

securely sending to said first entity in accordance with said first control, first audit information concerning use of said resource; and

securely sending to said second entity in accordance with said second control, second audit information concerning use of said resource, said second audit information being at least in part different from said first audit information.

395. A method for auditing the use of at least one resource with a secure operating environment, said method comprising:

securely receiving first and second control alternatives from an entity external to said operating environment;

selecting one of said first and second control alternatives;

using at least one resource;

if said first control alternative is selected by said selecting step, securely sending to said entity in accordance with said first control alternative, first audit information concerning use of said resource; and

if said second control alternative is selected by said selecting step, securely sending to said second entity in accordance with said second control alternative, second audit information concerning use of said resource, said second audit information being at least in part different from said first audit information.

396. A method and/or system for enabling a sale of protected digital information that has been previously distributed to users, the method or system being characterized by a secure element that selectively controls access to the protected digital information based on electronic controls associated with the information.

397. A distributed, secure electronic point of sale system or method characterized by a secure processing element for selectively releasing goods and/or services in exchange for compensation.

398. In a distributed digital network, an advertising method characterized by the steps of tracking usage of digital information that has associated with it one or more controls with respect to access to and/or usage of said information; and targeting advertising messages based at least in part on said tracking.

399. A distributed electronic advertising system characterized in that the system uses a distributed network of interoperable protected processing environments to at least in part deliver advertising to users.

400. A distributed, secure, virtual black box comprised of nodes located at VDE content container creators, other content providers, client users, and recipients of secure VDE content usage information) site, the nodes of said virtual black box including a secure subsystem having at least one secure hardware element such as a semiconductor element or other hardware module for securely executing VDE control processes, said secure subsystems being distributed at nodes along a pathway of information storage, distribution, payment, usage, and/or auditing.

401. A protected processing system or method providing multiple currencies and/or payment arrangements for the secure processing and releasing of protected digital information.

402. A distributed secure method or system characterized in that a user's age is used as a criteria for electronically, securely releasing information and/or resources to the user.

403. A method of renting an electronic appliance defining a secure processing environment.

404. A virtual distribution environment providing any one or more of the following features and/or elements and/or combinations thereof:

a configurable protected, distributed event management system; and/or

a trusted, distributed transaction and storage management arrangement; and/or

plural pathways for providing information, for control information, and/or for reporting; and/or

multiple payment methods; and/or

multiple currencies; and/or

EDI; and/or

Electronic banking; and/or

electronic document management; and/or

electronic secure communication; and/or

e-mail; and/or

distributed asynchronous reporting; and/or

combination asynchronous and online management; and/or

privacy control by users; and/or

testing; and/or

using age as a class; and/or

appliance control (renting, etc.); and/or

telecommunications infrastructure; and/or

games management; and/or

extraction of content from an electronic container; and/or

embedding of content into an electronic container; and/or

multiple certificate to allow for breach of a key; and/or

virtual black box; and/or

independence of control information from content; and/or

multiple, separate, simultaneous control sets for one digital information property; and/or

updating control information for already distributed digital information; and/or

organization information management; and/or

coupled external and organization internal chain of handling and control; and/or

a content usage consequence management system (reporting, payment, etc., multiple directions); and/or

a content usage reporting system providing differing audit information and/or reduction going to multiple parties holding rights in content; and/or

an automated remote secure object creation system; and/or

infrastructure background analysis to identify improper use; and/or

seniority of control information system; and/or

secure distribution and enforcement of rules and controls separately from the content they apply to; and/or

redistribution management by controlling the rights and/or number of copies and or pieces etc. that may be redistributed; and/or

an electronic commerce taxation system; and/or

an electronic shopping system; and/or

an electronic catalog system; and/or

a system handling electronic banking, electronic shopping, and electronic content usage management; and/or

an electronic commerce multimedia system; and/or

a distributed, secure, electronic point of sale system; and/or

advertising; and/or

electronics rights management; and/or

a distributed electronic commerce system; and/or

a distributed transaction system or environment; and/or

a distributed event management system; and/or

a distributed right systems.

405. A Virtual Distribution Environment substantially as shown in Figure 1.

406. An "Information Utility" substantially as shown in Figure 1A.

407. A chain of handling and control substantially as shown in Figure 1.

408. Persistent rules and control information substantially as shown in Figure 2A.

409. A method of providing different control information substantially as shown in Figure 1.

410. Rules and/or control information substantially as shown in Figure 4.

411. An object substantially as shown in Figures 5A and 5B.

412. A Secure Processing Unit substantially as shown in Figure 6.

413. An electronic appliance substantially as shown in Figure 7.

414. An electronic appliance substantially as shown in Figure 8.

415. A Secure Processing Unit substantially as shown in Figure 9.

416. A "Rights Operating System" ("ROS") architecture substantially as shown in Figure 10.

417. Functional relationship(s) between applications and the Rights Operating System substantially as shown in Figures 11A-11C.

418. Components and component assemblies substantially as shown in Figures 11D-11J.

419. A Rights Operating System substantially as shown in FIGURE 12.

420. A method of objection creation substantially as shown in Figure 12A.

421. A "protected processing environment" software architecture substantially as shown in Figure 13.

422. A method of supporting a channel substantially as shown in Figure 15.

423. A channel header and channel detail record substantially as shown in Figure 15 A.

424. A method of creating a channel substantially as shown in Figure 15B.

425. A secure data base substantially as shown in Figure 16.

426. A logical object substantially as shown in Figure 17.

427. A stationary object substantially as shown in FIGURE 18.

428. A travelling object substantially as shown in FIGURE 19.

429. A content object substantially as shown in FIGURE 20.

430. An administrative object substantially as shown in Figure 21.

431. A method core substantially as shown in Figure 22.

432. A load module substantially as shown in FIGURE 23.

433. A User Data Element (UDE) and/or Method Data Element (MDE) substantially as shown in FIGURE 24.

434. Map meters substantially as shown in FIGURES 25A-25C.

435. A permissions record (PERC) substantially as shown in FIGURE 26.

436. A permissions record (PERC) substantially as shown in FIGURES 26A and 26B.

437. A shipping table substantially as shown in FIGURE 27.

438. A receiving table substantially as shown in FIGURE 28.

439. An administrative event log substantially as shown in FIGURE 29.

440. A method of interrelating and using an object registration table, a subject table and a user rights table substantially as shown in Figure 30.

441. A method of using a site record table and a group record table to track portions of a secure database substantially as shown in FIGURE 34.

442. A process for updating a secure database substantially as shown in FIGURE 35.

443. A process of inserting new elements into a secure database substantially as shown in FIGURE 36.

444. A process of accessing elements in a secure database substantially as shown in FIGURE 37.

445. A process of protecting a secure database element substantially as shown in FIGURE 38.

446. A process of backing up a secure database substantially as shown in FIGURE 39.

447. A process of recovering a secure database substantially as shown in FIGURE 40.

448. A process of enabling performing reciprocal methods to provide a chain of handling and control substantially as shown in FIGURES 41A-41D.

449. A "reciprocal" BUDGET method substantially as shown in FIGURES 42A-42D.

450. A reciprocol audit method substantially as shown in FIGURES 44A-44C.

451. A method for controlling release of content or other method substantially as shown in any of FIGURES 45-48.

452. An event method substantially as shown in FIGURES 53A-53B.

453. A billing method substantially as shown in FIGURE 53C.

454. An extract method substantially as shown in FIGURE 57A.

455. An embed method substantially as shown in FIGURE 57A.

456. An obscure method substantially as shown in FIGURE 58A.

457. A fingerprint method substantially as shown in FIGURE 58B.

458. A fingerprint method substantially as shown in FIGURE 58C.

459. A meter method substantially as shown in FIGURE 6.

460. A key "convolution" process substantially as shown in FIGURE 62.

461. A process of generating different keys using a key convolution process to determine a "true" key substantially as shown in FIGURE 63.

462. A process of initializing protected processing environment keys substantially as shown in FIGURES 64 and/or 65.

463. A process for decrypting information contained within stationary objects substantially as shown in FIGURE 66.

464. A process for decrypting information contained within traveling objects substantially as shown in FIGURE 67.

465. A process for initializing a protected processing environment substantially as shown in FIGURE 68.

466. A process of downloading firmware into a protected processing environment substantially as shown in FIGURE 69.

467. Multiple VDE electronic appliances connected together with a network or other communications means substantially as shown in FIGURE 70.

468.A portable VDE electronic appliance substantially as shown in FIGURE 71.

469. "Pop-up" displays that may be generated by the user notification and exception interface substantially as shown in Figures 72A-72D.

470. A smart object substantially as shown in FIGURE 73.

471. A method of processing smart objects substantially as shown in FIGURE 74.

472. Electronic negotiation substantially as shown in any of FIGURES 75A-75D.

473. An electronic agreement substantially as shown in FIGURES 75E-75F.

474. Electronic negotiation processes substantially as shown in any of FIGURES 76A-76B.

475. A chain of handling and control substantially as shown in FIGURE 77.

476. A VDE "repository" substantially as shown in FIGURE 78.

477. A process of using a chain of handling and control to evolve and transform VDE managed content and control information substantially as shown in any or all of FIGURES 79-83.

478. A chain of handling and control involving several categories of VDE participants substantially as shown in FIGURE 84.

479. A chain of distribution and handling within an organization substantially as shown in FIGURE 85.

480. A chain of handling and control substantially as shown in Figures 86 and/or 86A.

481. A virtual silicon container model substantially as shown in Figure 87.

482. A method of business automation characterized by the steps of (a) creatings one or more secure containers including encrypted accounting and/or other administrative information content, (b) associating control information with one or more of such one or more secure containers including a description of (i) the one or more parties whom may use one or more of the one or more containers, and (ii) the operations that will be performed for one or more parties with respect to such accounting and/or other administrative information, (c) electronically delivering one or more of such one or more containers such to one or more parties, and (d) enabling through the use of a protected processing environment the enforcement of at least a portion of such control information.

483. A business automation system characterized by:

means for providing at least one secure container including administrative information content having control information associated therewith, and

a protected processing environment for enforcing, at least in part, the control information.

484. A business automation system comprising (a) distributed, interoperable protected processing environment installations, (b) secure containers for distribution of digital

information, (c) control information supporting the automation of chain of handling and control functions.

485. A method of business automation characterized by the steps of providing interoperable protected processing environment nodes to plural parties, communicating first encrypted digital information from a first party to a second party, communicating second encrypted digital information including at least a portion of said first communicated digital information and/or information related to the use of said first digital information, to a third party different from said first or second parties, wherein use of said second encrypted digital information is regulated, at least in part, by an interoperable protected processing environment available to said third party.

486. A business automation system characterized by:

plural protected processing environment nodes,

means for communicating digital information between the nodes, and

wherein at least one of the nodes includes means for regulating the use of said communicated digital information.

487. A method for chain of handling and control characterized by the steps of (a) a first party placing protected digital information into a first software container and stipulating

rules and controls governing use of at least a portion of said digital information, (b) providing said software container to a second party, wherein said second party places said software container into a further software container and stipulates rules and controls for at least in part managing use of at least a portion of said digital information and/or said first software container by a third party.

488. A chain of handling and control system characterized by:

means for placing digital information into a first software container and for stipulating rules and/or controls governing use of at least a portion of said digital information, and

means for placing said software container into a further software container and for stipulating further rules and/or controls for at least in part managing use of at least a portion of said digital information and/or said first software container.

489. A system for chain of handling and control including (a) a first container containing at least in part protected digital information, (b) at least in part protected control information stipulated by a first party establishing conditions for use of at least a portion of said digital content, (c) a second container different from said first container, said second container containing said first container, (d) control information stipulated

independently by a second party for at least in part setting conditions for managing use of the contents of said second container.

490. A system for electronic advertising including: (a) means to provide digital information to users for their use, (b) means to provide advertising content to said users in combination with said digital information, (c) means to audit use of said digital information, (d) means to securely acquire usage information regarding use of advertising content, (e) means to securely report information based upon said advertising content usage information, (f) compensating at least one content provider at least in part based upon use of said advertising content.

491. A method for electronic advertising characterized by the steps of (a) placing digital information into a container, (b) associating advertising information with at least a portion of said digital information, (c) securely providing said container to a container user, (d) monitoring user viewing of advertising information, and (d) receiving payment from an advertiser, wherein said payment is related to user viewing of said advertising information.

492. A system for electronic advertising involving (a) means to containerize digital information including both content

and advertising information, (b) means to monitor viewing of at least a portion of said advertising information, (c) means to charge for user viewing of at least a portion of said advertising information, (d) means to securely communicate information based upon said viewing in a secure container, and (e) control information related to said containerized digital information for managing the communication of said information based upon said viewing.

493. A method for electronic advertising characterized by the steps of (a) containerizing digital information including both content and advertising information, (b) monitoring user viewing of at least a portion of said advertising information, (c) charging for user viewing of at least a portion of said advertising information, (d) securely communicating information based upon said viewing in a secure container, and (e) at least in part managing, through the use of control information related to said advertising information, the communication of information based upon said viewing.

494. A method of clearing transaction information characterized by the steps of (a) securely distributing digital information to a first user of an interoperable protected processing environment, (b) securely distributing further digital information to a user of an interoperable protected processing

environment different from said at first user (c) receiving information related to usage of said digital information, (d) receiving information related to usage of said further digital information, and (e) processing information received according to steps (c) and (d) to perform at least one of (I) an administrative, or (II) an analysis, function.

495. A system for clearing transaction information including (a) a first container containing at least in part protected digital information and associated control information, (b) a second secure container containing further at least in part protected digital information and associated control information, (c) means to distribute said first and second containers to users, (d) communication means for communicating information at least in part derived from user usage of said first container digital information, (e) communication means for communicating information at least in part derived from user usage of said second container digital information, (f) processing means at a clearinghouse site for receiving the information communicated through steps (d) and (e), wherein said processing means perform administrative and/or analysis processing of at least a portion of said communicated information.

496. A method for clearinghouse analysis characterized by the steps of: (a) enabling plural independent clearinghouses for

administrating and/or analyzing usage of distributed, at least in part protected, digital information, (b) providing interoperable protected processing environments to plural, independent users, and (c) enabling a user to select a clearinghouse for use with an interoperable protected processing environment

497. A system for clearinghouse analysis including (a) plural independent clearinghouses for administrating and/or analyzing usage of distributed, at least in part protected, digital information, (b) at least one interoperable protected processing environments at each of plural user locations, (c) selecting means for enabling a user to select one of said plural independent clearinghouse to perform payment and/or analysis functions related to the use of at least a portion of said at least in part protected, digital information.

498. A method of electronic advertising characterized by the steps of

creating one or more electronic advertisements, creating one or more secure containers including at least a portion of such advertisements,

associating control information with such advertisements including control information describing at least one of: (a) reporting at least some advertisement usage information to one or more content providers, advertisers and/or agents, (b)

providing one or more credits to a user based on such user's viewing and/or other usage of such advertisements, (c) reporting advertisement usage information to one or more market analysts, (d) providing a user with ordering information for and/or means for ordering one or more products and/or services, and/or (e) providing one or more credits to a content provider based on one or more users' viewing and/or other usage of such advertisements,

providing such containers and such control information to one or more users,

enabling such users to use such containers at least in part in accordance with such control information.

499. A system for electronic advertising including (a) means to provide digital information to users for their use, (b) means to provide advertising content to said users in combination with said digital information, (c) means to audit use of said digital information, (d) means to acquire usage information regarding use of advertising content, (e) means to securely report information based upon said advertising content usage information, and (f) compensating at least one content provider at least in part based upon use of such advertising content.

500. A system for chain of handling and control including (a) a first container containing at least in part protected digital information, (b) at least in part protected control information stipulated by a first party establishing condition for use of at least a portion of said digital content, (c) a second container different from said first container, said second container containing said first container, and (d) control information stipulated independently by a second party for at least in part setting conditions for managing use of the contents of said second container.

501. A method of operating a clearinghouse characterized by the steps of receiving usage information related at least in part to use of secure containers from plural parties, determining payments due to one or more parties based at least in part on such usage information, performing and/or causing to be performed transactions resulting in payments to such parties based at least in part on such determinations.

502. An electronic clearinghouse comprising:

means for receiving usage information related at least in part to use of secure containers from plural parties,

means for determining payments due to one or more parties based at least in part on such usage information,

means for performing and/or causing to be performed transactions resulting in payments to such parties based at least in part on such determinations.

503. A method of operating a clearinghouse characterized by the steps of receiving usage information related at least in part to use of secure containers from plural parties, determining reports of usage for one or more parties based at least in part on such usage information, creating and/or causing to be created reports of usage based at least in part on such determination, delivering at least one of such reports to at least one of such parties.

504. A method of operating a clearinghouse characterized by the steps of receiving permissions and/or other control information from one or more content providers including information that enables delivery of at least one right in at least one secure container to other parties, receiving requests from plural parties for one or more rights in one or more secure containers, delivering permissions and/or other control information to such parties based at least in part on such requests.

505. A method of operating a clearinghouse characterized by the steps of receiving information from one or more parties

establishing a party's identity information, creating one or more electronic representations of at least a portion of such identity information for use in enabling and/or withholding at least one right in at least one secure container, performing an operation to certify such electronic representations, delivering such electronic representations to such party.

506. A method of operating a clearinghouse characterized by the steps of receiving a request for credit from a party for use with secure containers, determining an amount of credit based at least in part on such request, creating control information related to such an amount, delivering such control information to such user, receiving usage information related to use of such credit, performing and/or causing to be performed at least one transaction associated with collecting payment from such user.

507. A method for contributing secure control information with respect to an electronic value chain wherein control information is contributed by a party not directly participating in said value chain, comprising steps of: aggregating said contributed control information with control information associated with digital information stipulated by one or more parties in an electronic value chain, said aggregate control information at least in part managing conditions related to the use of at least a portion of said digital information.

508. A method for entering the payment of taxes associated with commercial events wherein secure control information for automatically governing tax payments for said commercial events is contributed by a party comprising steps of: aggregating said secure control information with control information that has been contributed by a separate party and controlling at least one condition for use of digital information.

509. A method for general purpose reusable electronic commerce arrangement characterized by the steps of:

(a) providing component structures, modular methods that can be configured together to comprise event controlled

(b) providing integrateable protected processing environments to plural independent users;

(c) employing secure communications means for communicating digital control information between integrateable protected processing environments; and

(d) enabling database managers operably connected to said processing environments for storing at least a portion of said provided component modular methods.

510. A system for general purpose, reusable electronic commerce including:

(a) component modular methods configured together to comprise event control structures;

(b) at least one interoperable processing environment at each of plural independent user locations;

(c) secure communications means for communicating digital control information between interoperable protected processing environments; and

(d) secured database managers operably connected to said protected processing environments for storing at least a portion of said component modular methods.

511. A general purpose electronic commerce credit system including:

(a) a secure interoperable protected processing environment;

(b) general purpose credit control information for providing credit for user usage of at least in part protected digital information; and

(c) at least in part protected digital information related control information for providing necessary information for employing credit through the use, at least in part, of said general purpose credit control information.

512. A method for enabling a general purpose electronic commerce credit system including:

(a) providing secure interoperable protected processing environments;

(b) supplying general purpose credit control information for providing credit for user usage of at least in part protected digital information; and

(c) providing, at least in part, protected digital information related control information for providing necessary information for employing credit through the use, at least in part, of said general purpose credit control information.

513. A document management system comprising one or more electronic appliances containing one or more SPUs and one or more secure databases operatively connected to at least one of the SPUs.

514. An electronic contract system comprising one or more electronic appliances containing one or more SPUs and one or more secure databases operatively connected to at least one of the SPUs.

515. An electronic appliance containing at least one SPU and at least one secure database operatively connected to at least one of the SPU(s).

516. An electronic appliance containing one or more CPUs where at least one of the CPUs is integrated with at least one SPU.

517. An electronic appliance containing one or more video controllers where at least one of the video controllers is integrated with at least one SPU.

518. An electronic appliance containing one or more network communications means where at least one of the network communications means is integrated with at least one SPU.

519. An electronic appliance containing one or more modems where at least one of the modems is integrated with at least one SPU.

520. An electronic appliance containing one or more CD-ROM devices where at least one of the CD-ROM devices is integrated with at least one SPU.

521. An electronic appliance containing one or more set-top controllers where at least one of the set-top controllers is integrated with at least one SPU.

522. An electronic appliance containing one or more game systems where at least one of the game systems is integrated with at least one SPU.

523. An integrated circuit supporting multiple encryption algorithms comprising at least one microprocessor, memory, input/output means, at least one circuit for encrypting and/or decrypting information and one or more software programs for use with at least one of the microprocessors to perform encryption and/or decryption functions.

524. An integrated circuit comprising at least one microprocessor, memory, at least one real time clock, at least one random number generator, at least one circuit for encrypting and/or decrypting information and independently delivered and/or independently deliverable certified software.

525. An integrated circuit comprising at least one microprocessor, memory, input/output means, a tamper resistant barrier and at least a portion of a Rights Operating System.

526. An integrated circuit comprising at least one microprocessor, memory, input/output means, at least one real time clock, a tamper resistant barrier and means for recording interruption of power to at least one of the real time clocks.

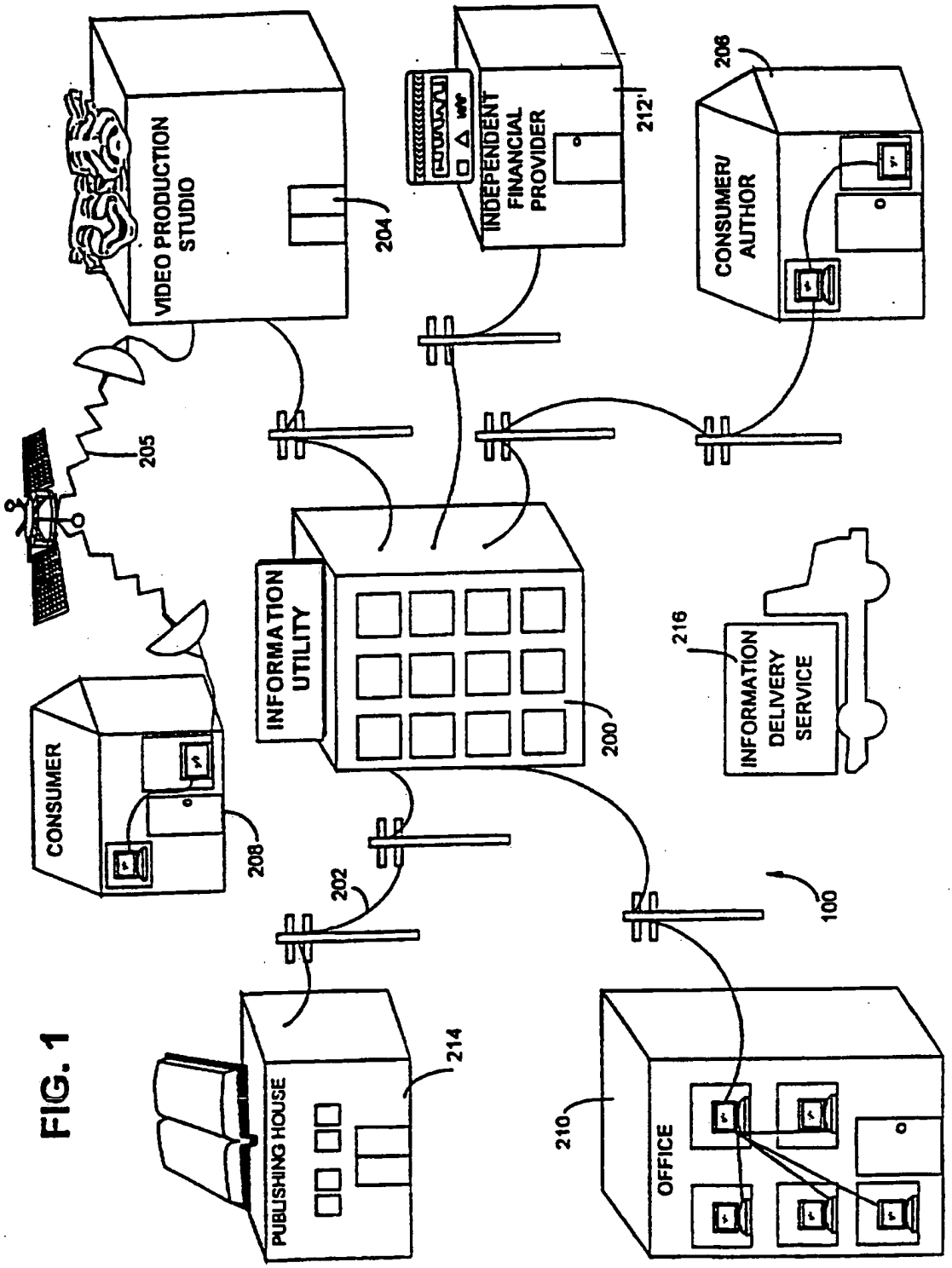

VIDEO PRODUCTION STUDIO
204
INDEPENDENT FINANCIAL PROVIDER
212
CONSUMER/ AUTHOR
206
205
INFORMATION UTILITY
200
INFORMATION DELIVERY SERVICE
216
CONSUMER
208
202
100
PUBLISHING HOUSE
214
OFFICE
210

FIG. 1

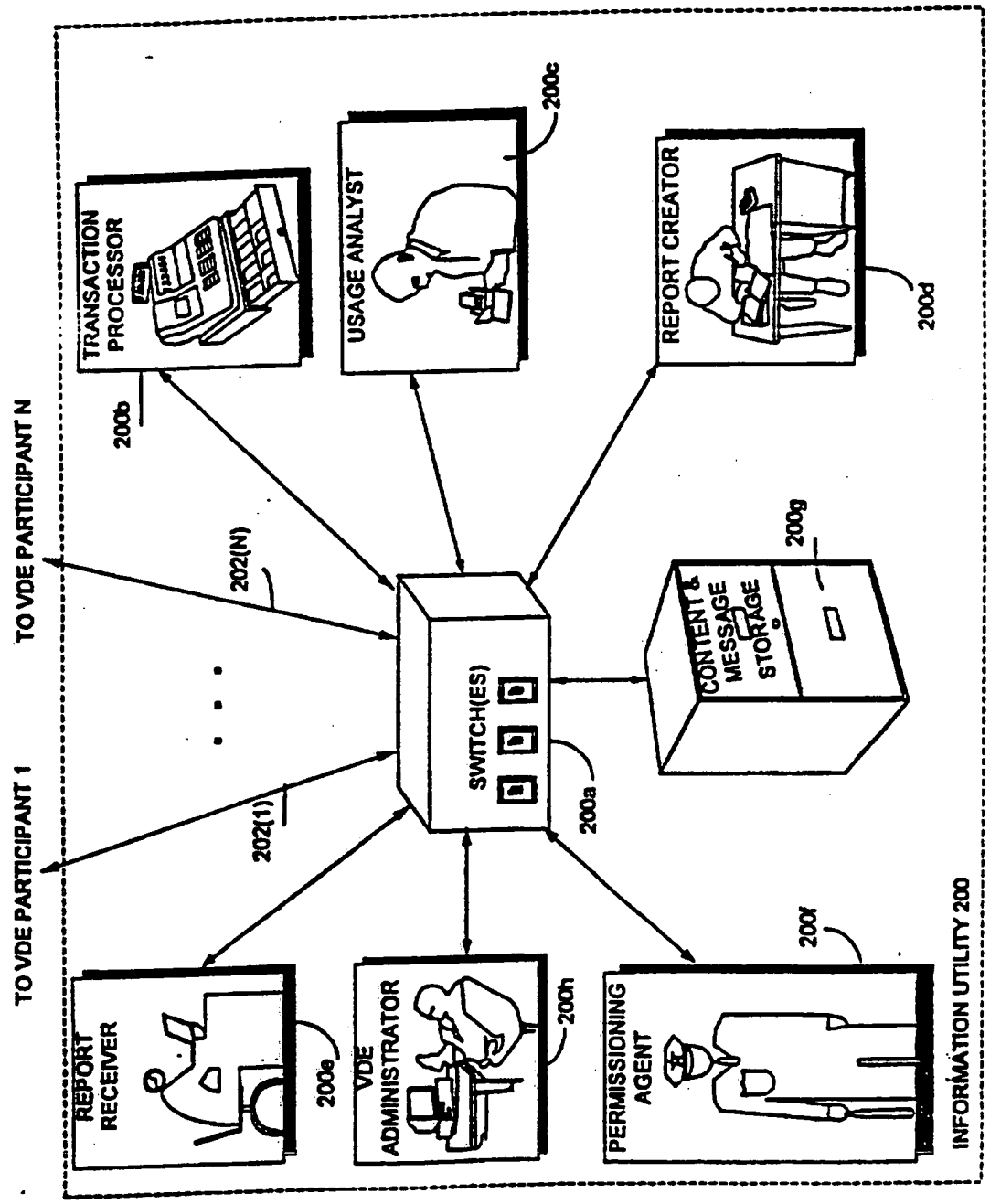

TO VDE PARTICIPANT 1
TO VDE PARTICIPANT N
202(1)
202(N)
SWITCH(ES)
200a
TRANSACTION PROCESSOR
200b
USAGE ANALYST
200c
REPORT CREATOR
200d
CONTENT & MESSAGE STORAGE
200g
REPORT RECEIVER
200e
VDE ADMINISTRATOR
200h
PERMISSIONING AGENT
200f
INFORMATION UTILITY 200

FIG. 1A

FIG. 2

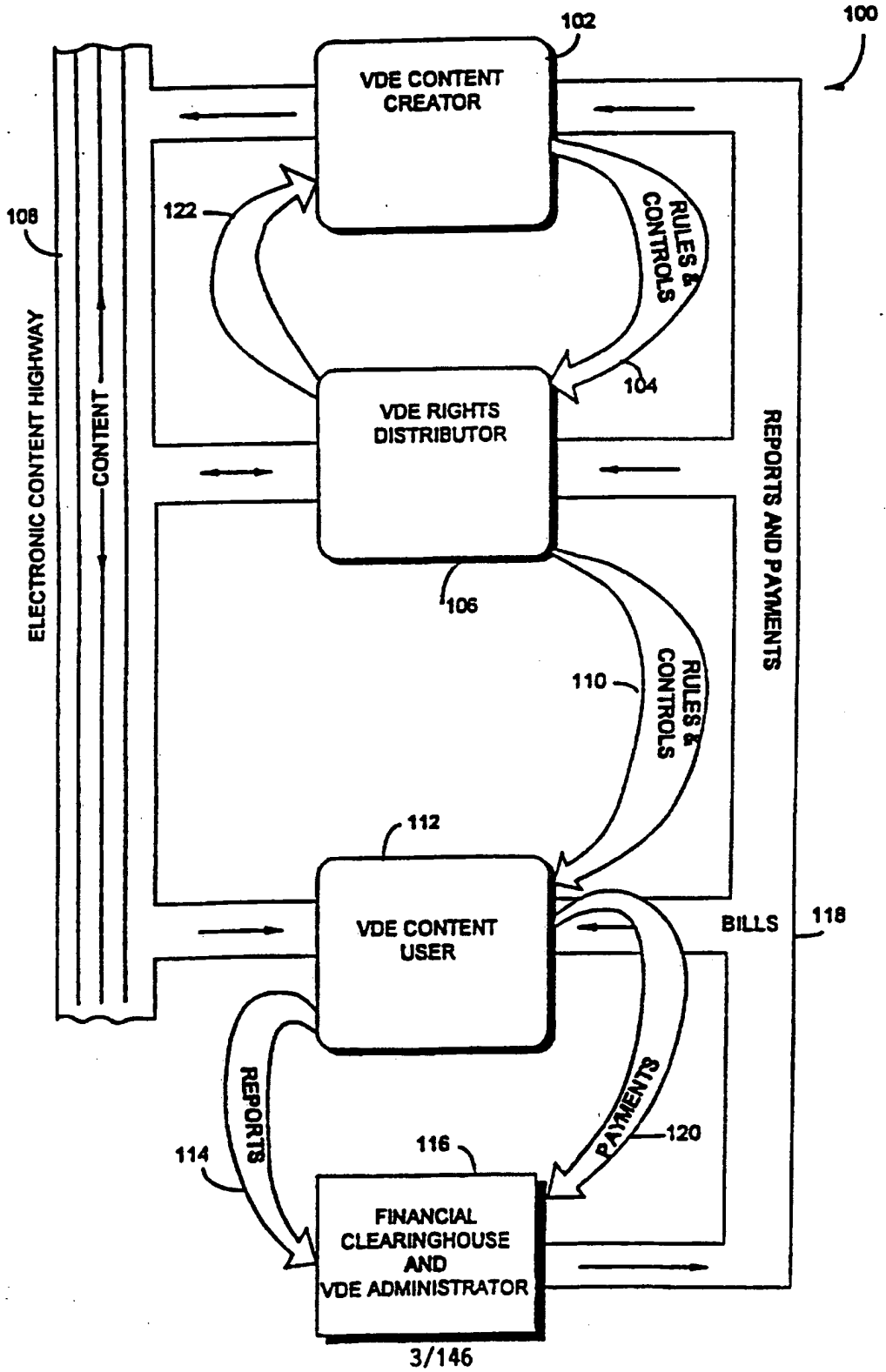

100
102
VDE CONTENT CREATOR
122
RULES & CONTROLS
104
108
ELECTRONIC CONTENT HIGHWAY
CONTENT
VDE RIGHTS DISTRIBUTOR
106
REPORTS AND PAYMENTS
110
RULES & CONTROLS
112
VDE CONTENT USER
BILLS
118
REPORTS
114
PAYMENTS
120
116
FINANCIAL CLEARINGHOUSE AND VDE ADMINISTRATOR

FIG. 2A

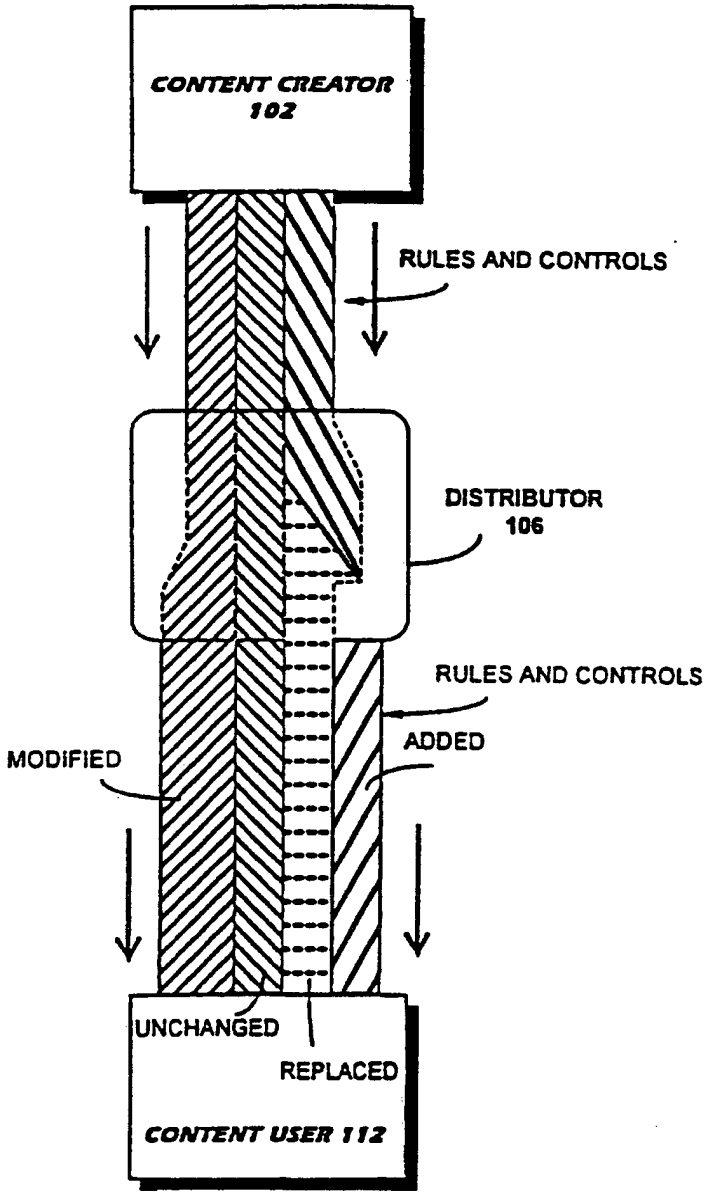
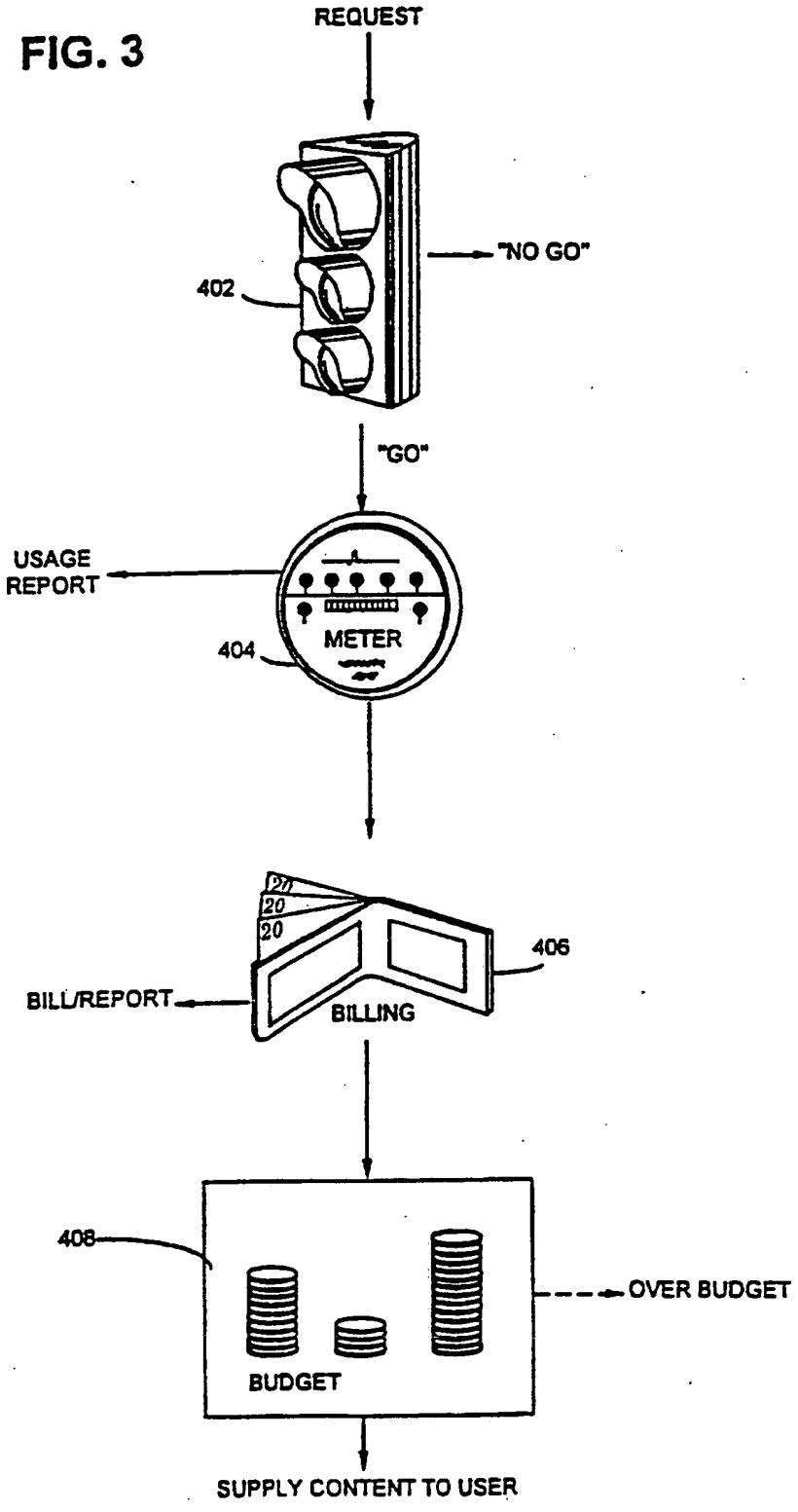

CONTENT CREATOR
102
RULES AND CONTROLS
DISTRIBUTOR
106
RULES AND CONTROLS
ADDED
MODIFIED
UNCHANGED
REPLACED
CONTENT USER 112

FIG. 3


REQUEST
"NO GO"
402
"GO"
USAGE REPORT
METER
404
406
BILL/REPORT
BILLING
408
OVER BUDGET
BUDGET
SUPPLY CONTENT TO USER

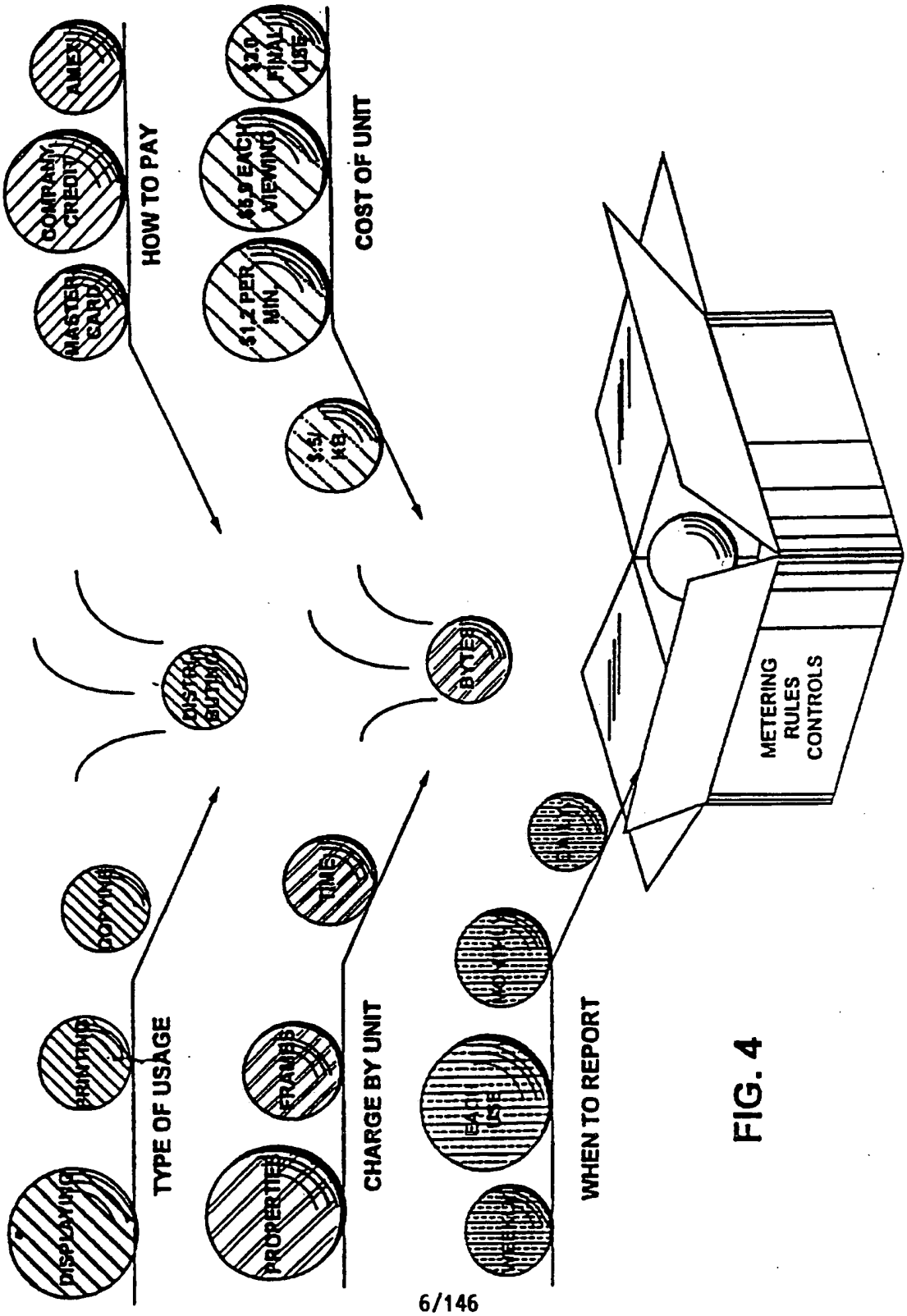
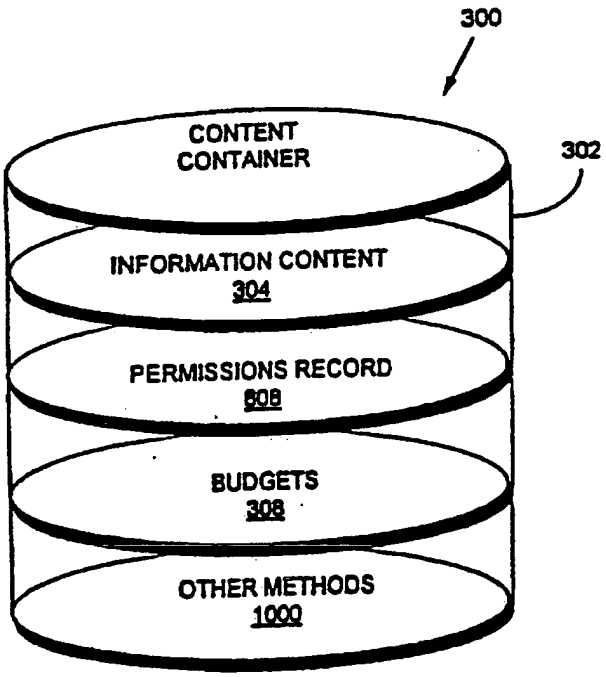

HOW TO PAY
COST OF UNIT
TYPE OF USAGE
CHARGE BY UNIT
WHEN TO REPORT
METERING
RULES
CONTROLS

FIG. 4

FIG. 5A


300
CONTENT CONTAINER
302
INFORMATION CONTENT 304
PERMISSIONS RECORD 808
BUDGETS 308
OTHER METHODS 1000

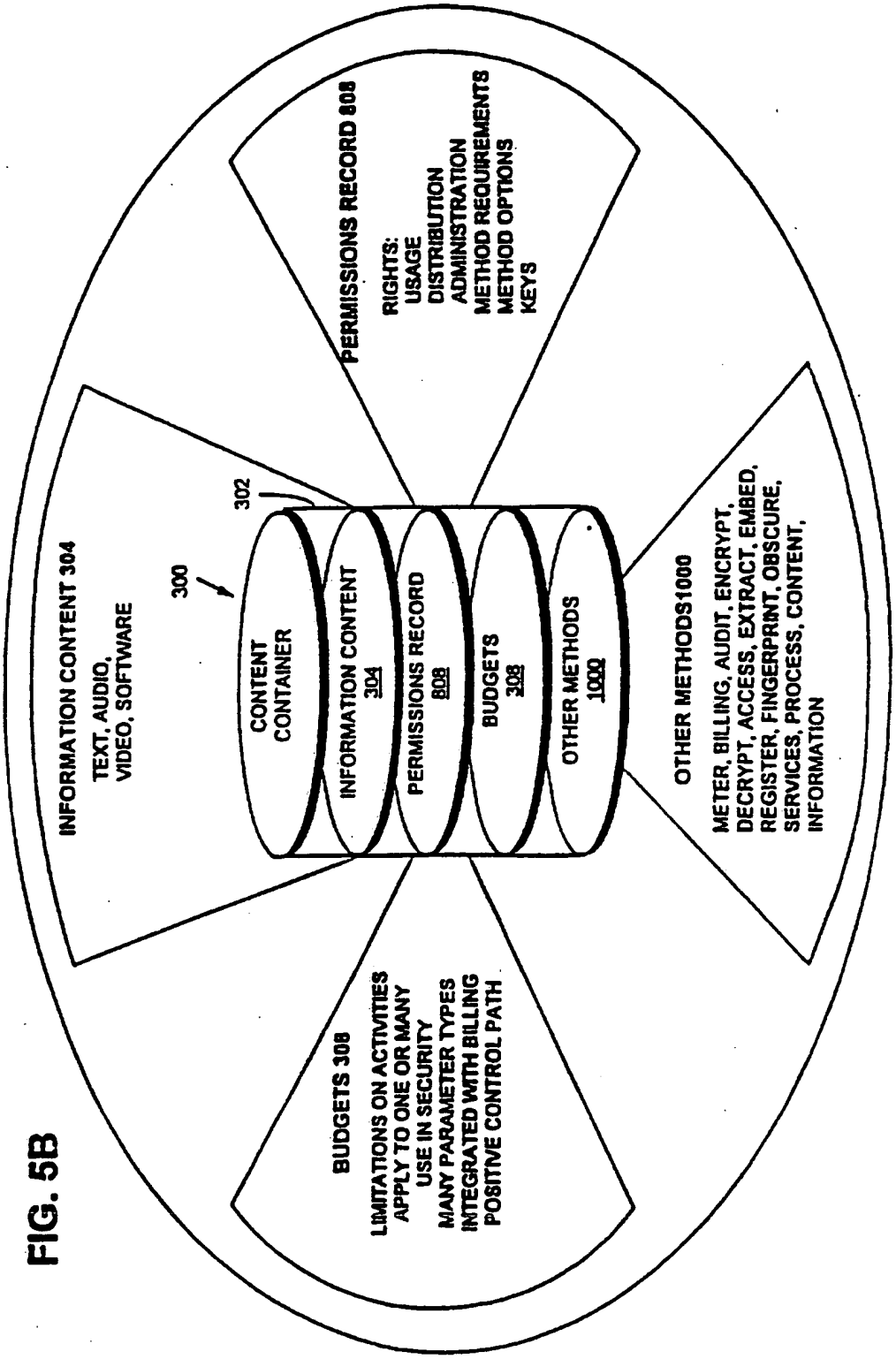
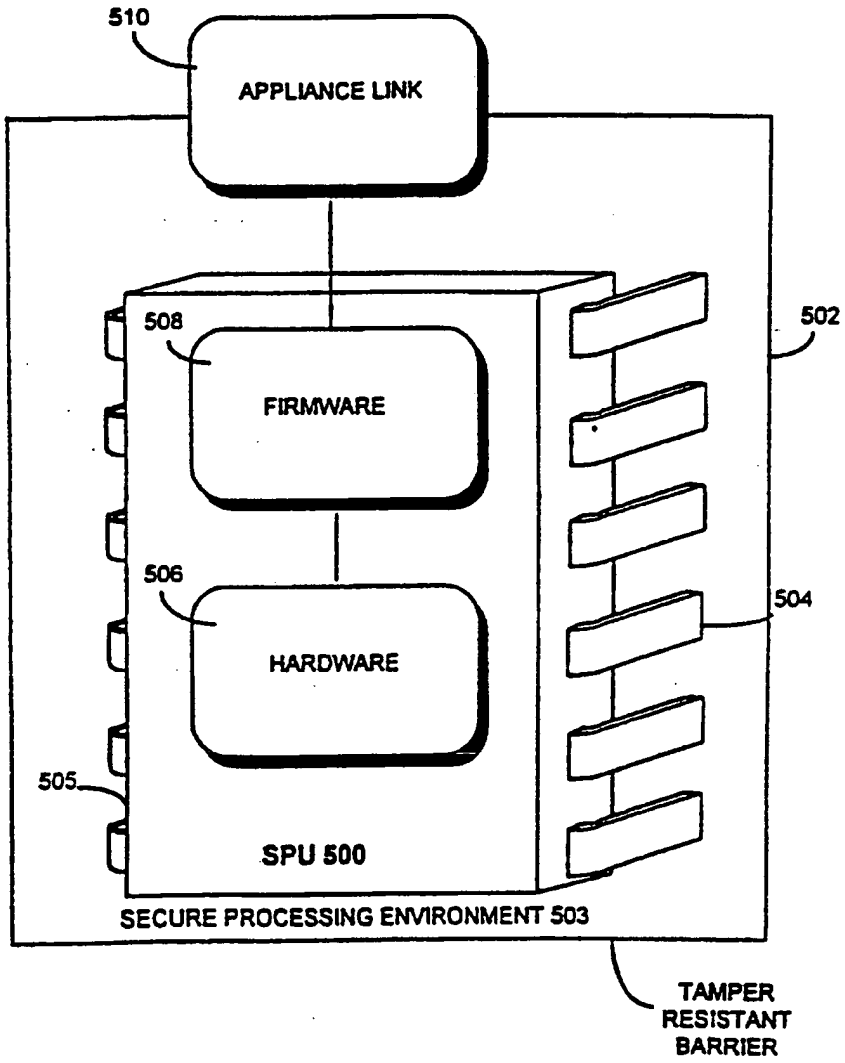

INFORMATION CONTENT 304
TEXT, AUDIO,
VIDEO, SOFTWARE
300
302
CONTENT
CONTAINER
INFORMATION CONTENT
304
PERMISSIONS RECORD
808
BUDGETS
308
OTHER METHODS
1000
PERMISSIONS RECORD 808
RIGHTS:
USAGE
DISTRIBUTION
ADMINISTRATION
METHOD REQUIREMENTS
METHOD OPTIONS
KEYS
OTHER METHODS1000
METER, BILLING, AUDIT, ENCRYPT,
DECRYPT, ACCESS, EXTRACT, EMBED,
REGISTER, FINGERPRINT, OBSCURE,
SERVICES, PROCESS, CONTENT,
INFORMATION
BUDGETS 308
LIMITATIONS ON ACTIVITIES
APPLY TO ONE OR MANY
USE IN SECURITY
MANY PARAMETER TYPES
INTEGRATED WITH BILLING
POSITIVE CONTROL PATH

FIG. 5B

FIG. 6


510
APPLIANCE LINK
508
FIRMWARE
506
HARDWARE
505
SPU 500
502
504
SECURE PROCESSING ENVIRONMENT 503
TAMPER RESISTANT BARRIER

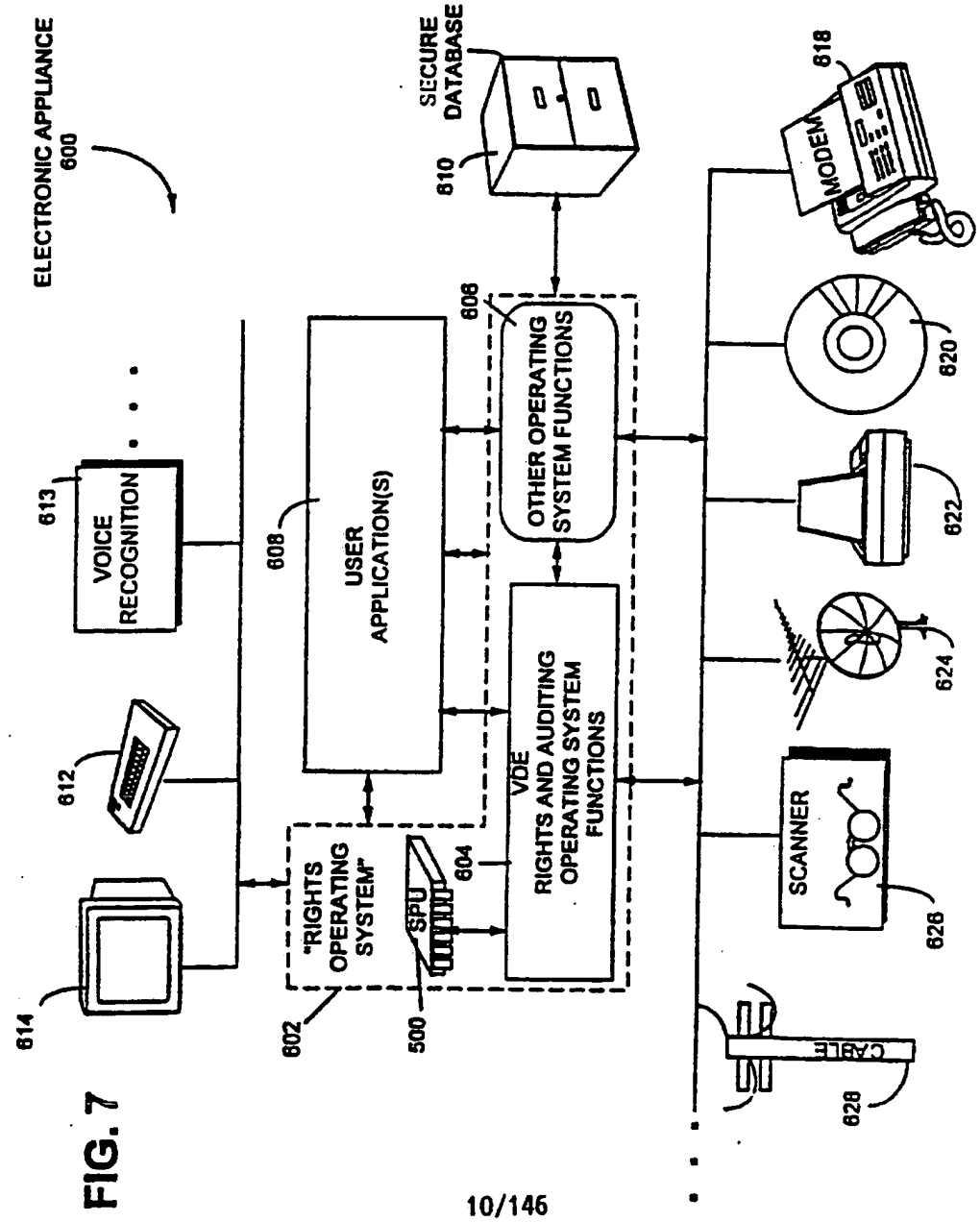
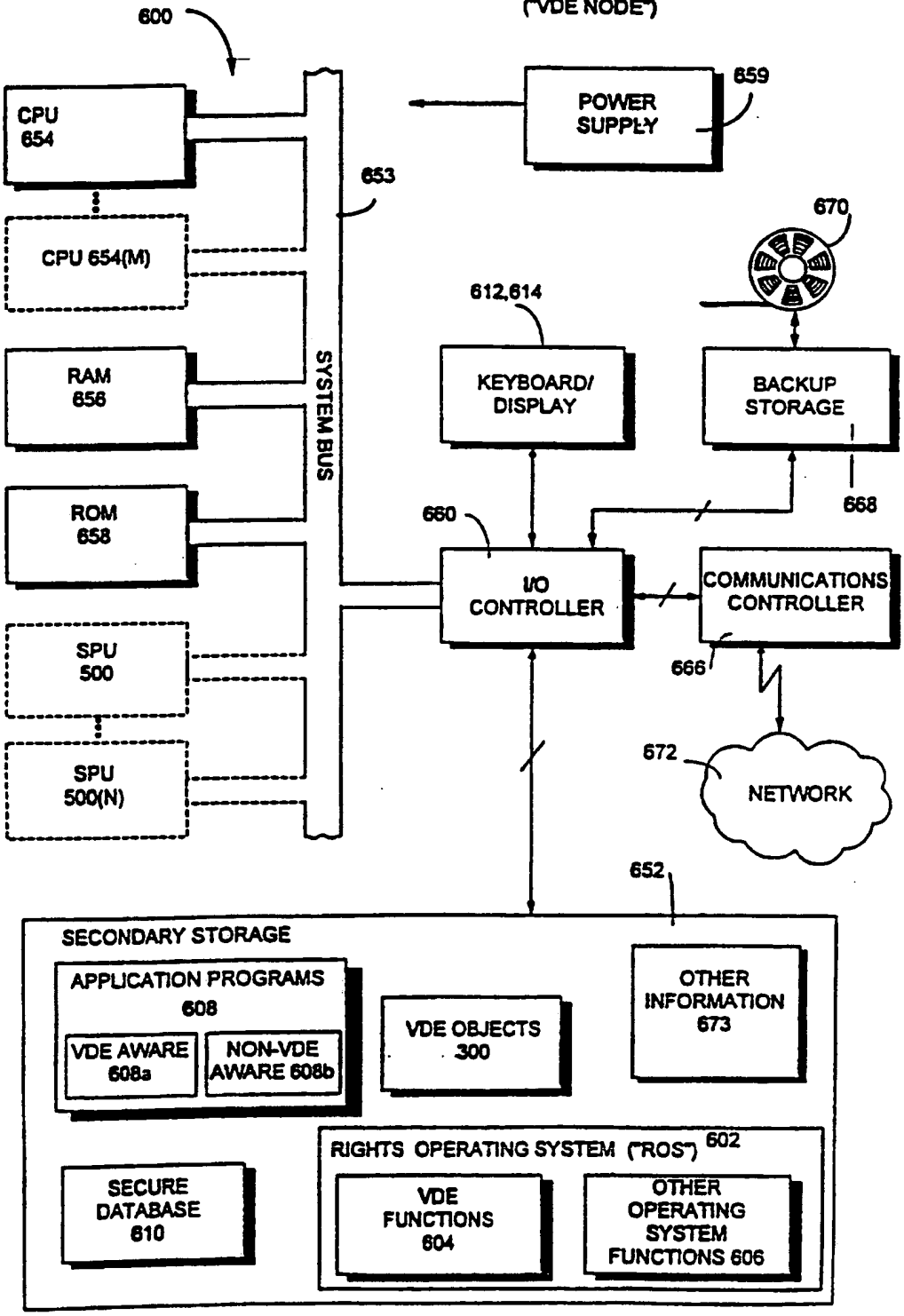

ELECTRONIC APPLIANCE
600
SECURE DATABASE
610
MODEM
618
613
VOICE RECOGNITION
608
USER APPLICATION(S)
606
OTHER OPERATING SYSTEM FUNCTIONS
820
622
612
624
"RIGHTS OPERATING SYSTEM"
SPU
604
VDE RIGHTS AND AUDITING OPERATING SYSTEM FUNCTIONS
SCANNER
626
614
602
500
CABLE
628

FIG. 7

FIG. 8 ELECTRONIC APPLIANCE 600 ("VDE NODE")



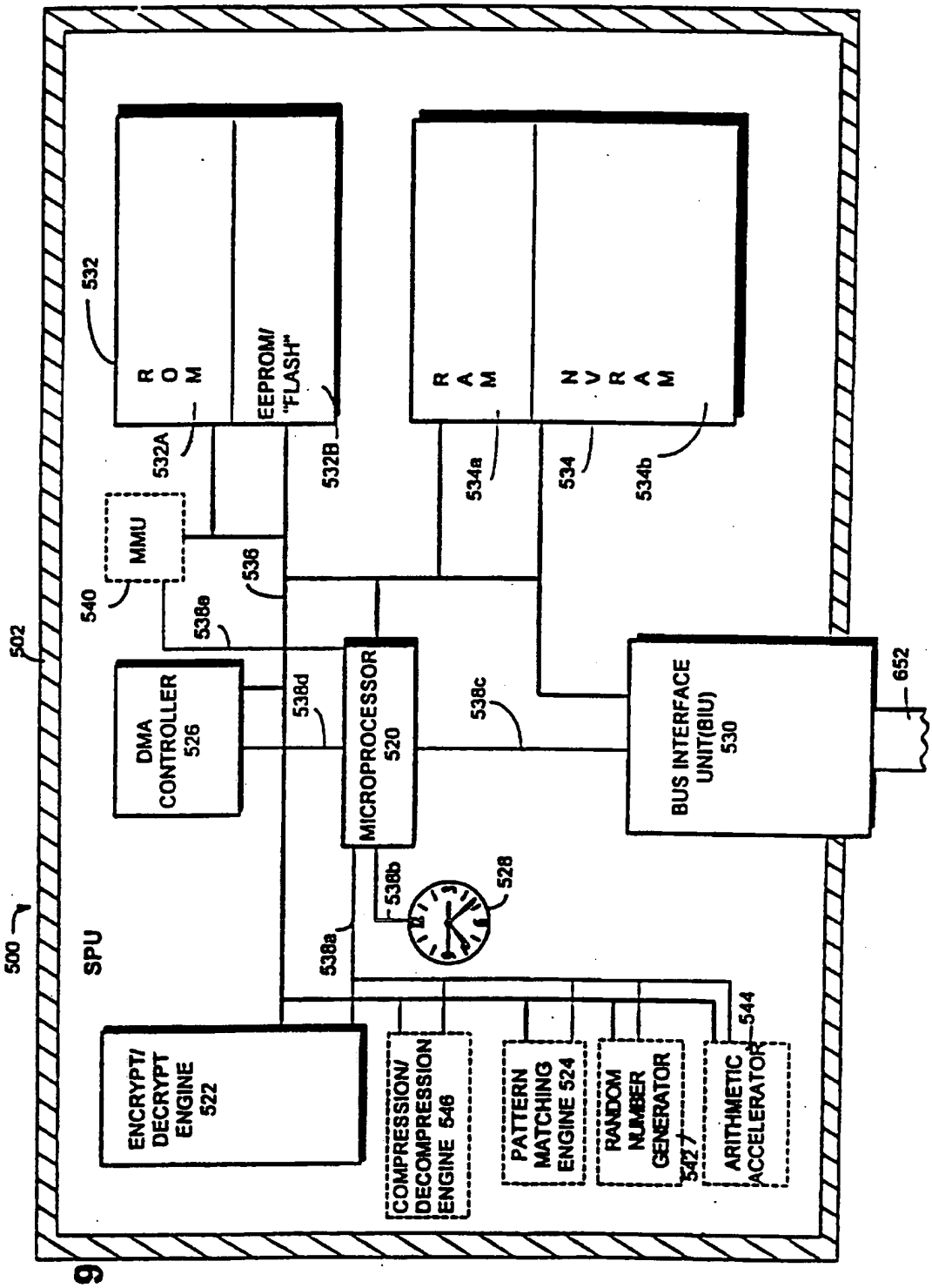

500
SPU
502
ROM
EEPROM/ "FLASH"
532
532A
532B
RAM
NVRAM
534a
534
534b
MMU
540
536
538e
DMA CONTROLLER 526
538d
MICROPROCESSOR 520
538c
BUS INTERFACE UNIT(BIU) 530
652
538b
528
538a
ENCRYPT/ DECRYPT ENGINE 522
COMPRESSION/ DECOMPRESSION ENGINE 546
PATTERN MATCHING ENGINE 524
RANDOM NUMBER GENERATOR 527
ARITHMETIC ACCELERATOR 544

FIG. 9

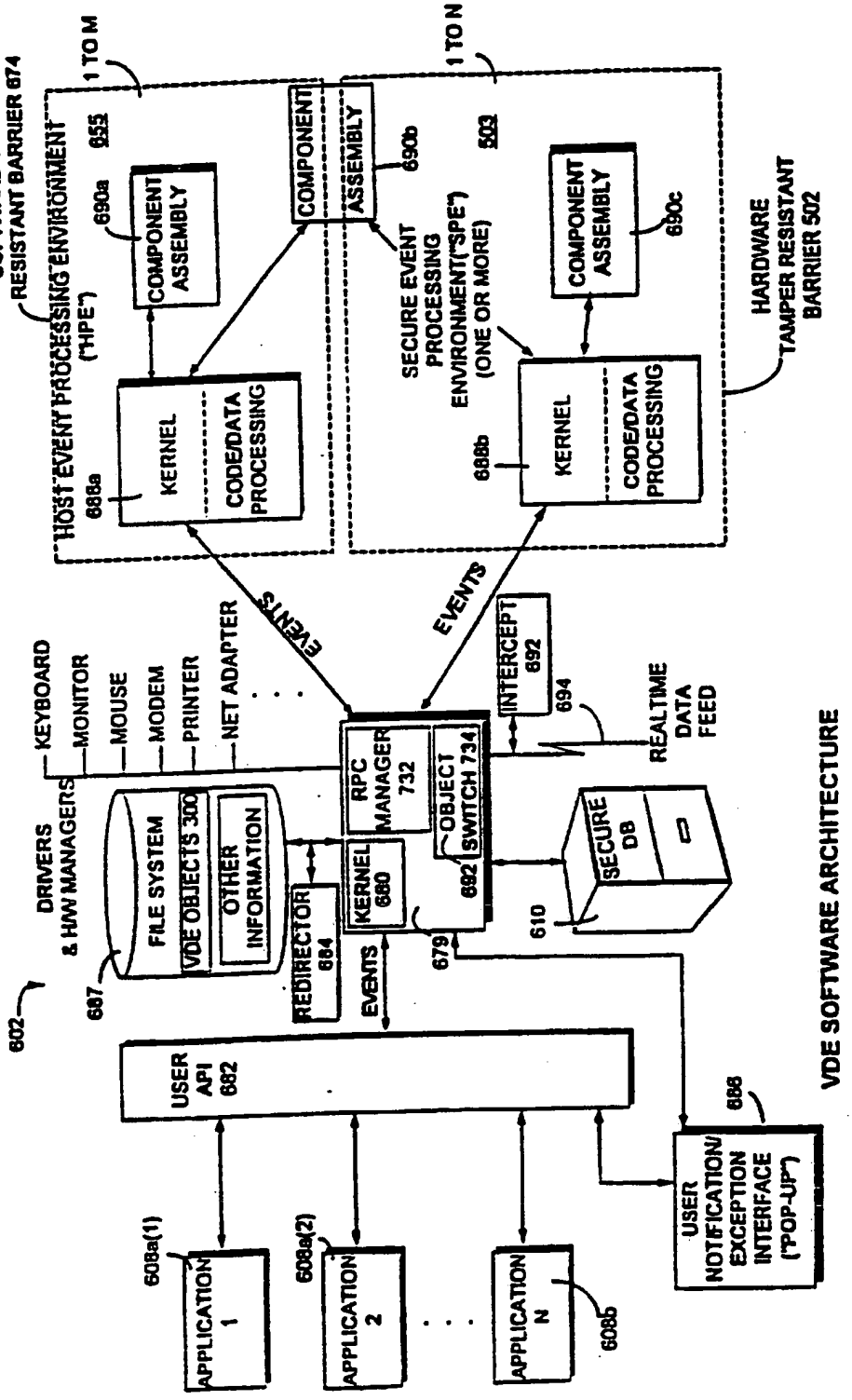

SOFTWARE TAMPER RESISTANT BARRIER 674
HOST EVENT PROCESSING ENVIRONMENT ("HPE")
1 TO M
955
690a
COMPONENT ASSEMBLY
COMPONENT
ASSEMBLY
690b
1 TO N
503
SECURE EVENT PROCESSING ENVIRONMENT("SPE") (ONE OR MORE)
COMPONENT ASSEMBLY
690c
HARDWARE TAMPER RESISTANT BARRIER 502
688a
KERNEL
CODE/DATA PROCESSING
688b
KERNEL
CODE/DATA PROCESSING
EVENTS
EVENTS
KEYBOARD
MONITOR
MOUSE
MODEM
PRINTER
NET ADAPTER
INTERCEPT 692
694
REALTIME DATA FEED
DRIVERS & HW MANAGERS
RPC MANAGER 732
OBJECT SWITCH 734
692
FILE SYSTEM
VDE OBJECTS 300
OTHER INFORMATION
687
KERNEL 680
REDIRECTOR 684
EVENTS
679
SECURE DB
610
602
USER API 682
686
USER NOTIFICATION/ EXCEPTION INTERFACE ("POP-UP")
608a(1)
APPLICATION 1
608a(2)
APPLICATION 2
APPLICATION N
608b
VDE SOFTWARE ARCHITECTURE

FIG. 10

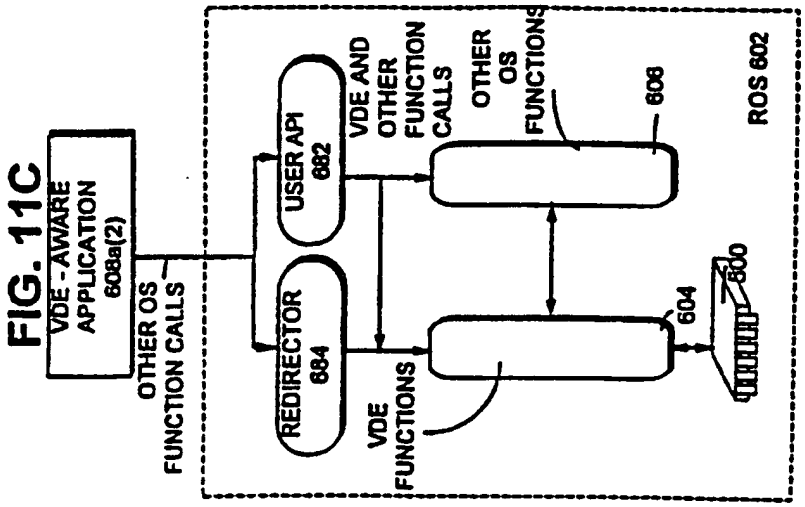


FIG. 11C

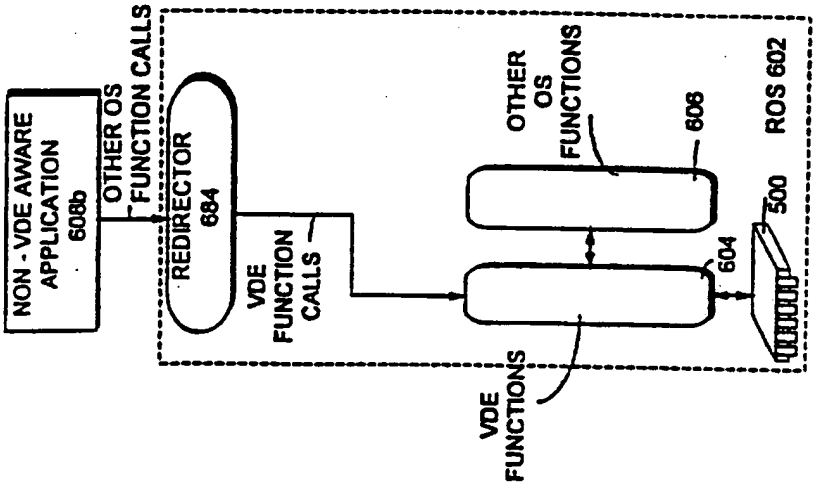


FIG. 11B

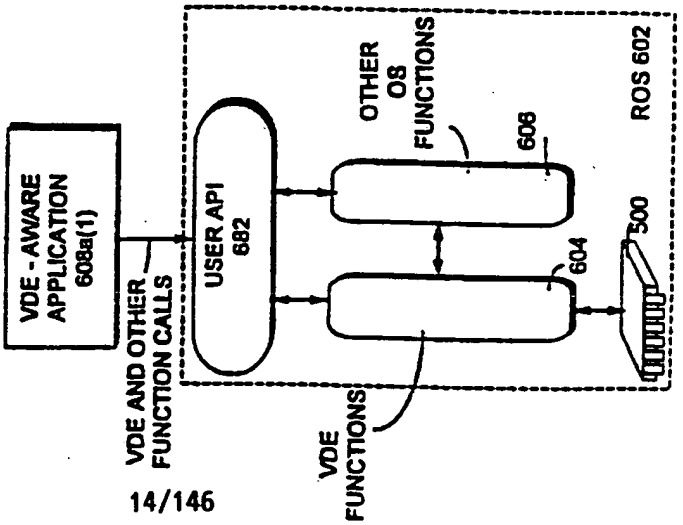


FIG. 11A

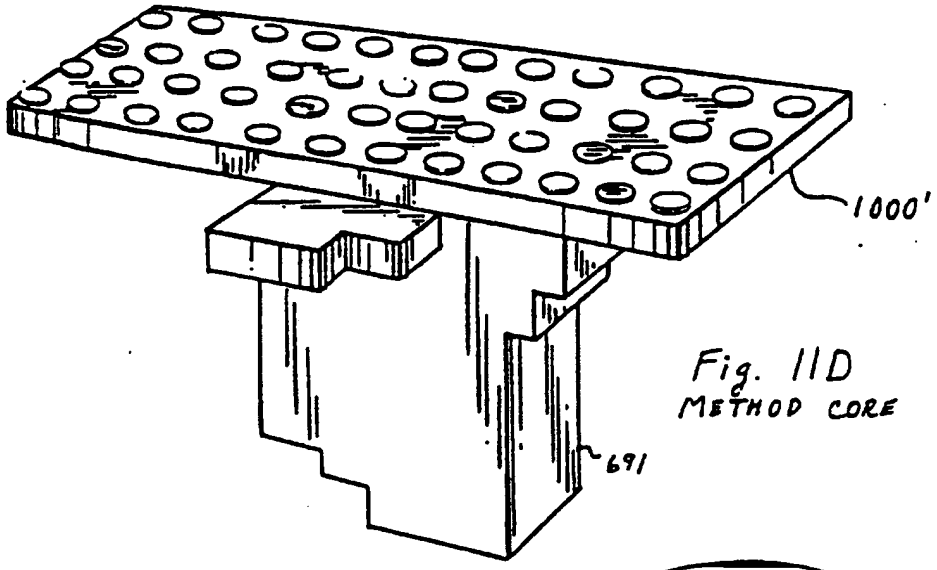
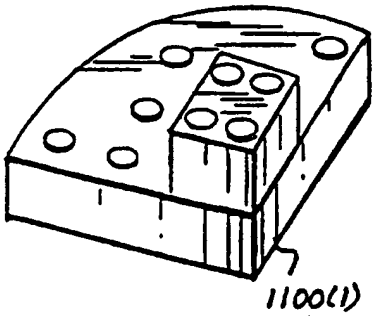


Fig. 11D
METHOD CORE



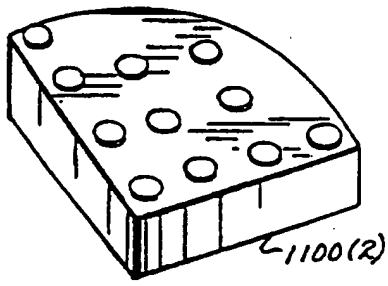


Fig. 11F
LOAD MODULE

Fig. 11E
LOAD MODULE
WITH DTD

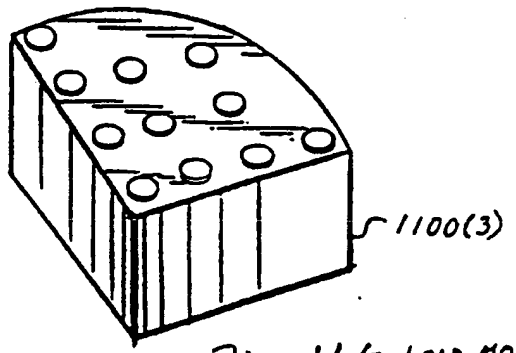


Fig 11G LOAD MODULE

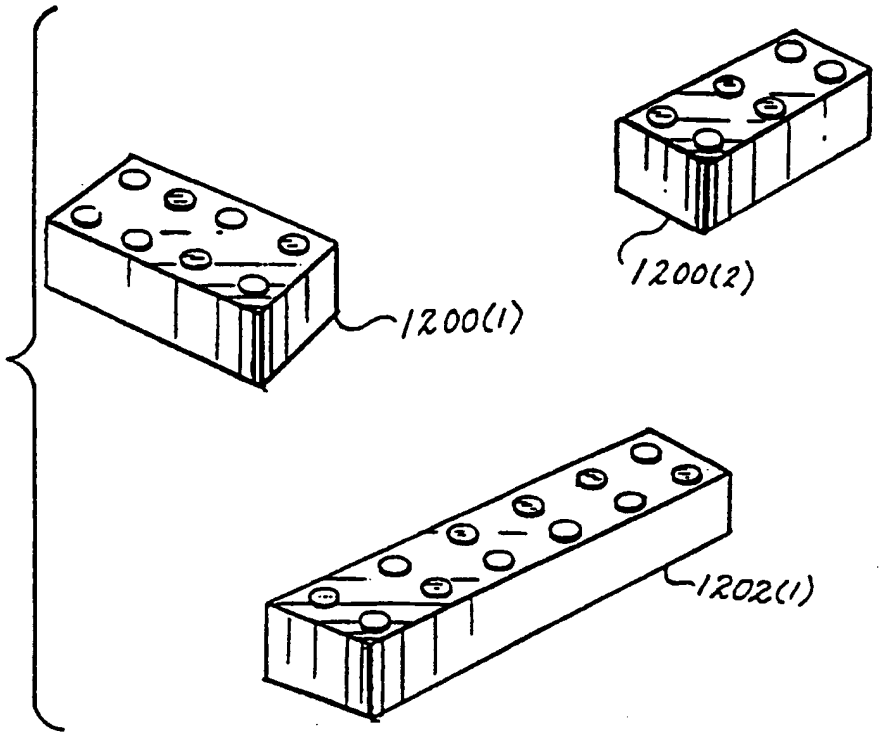
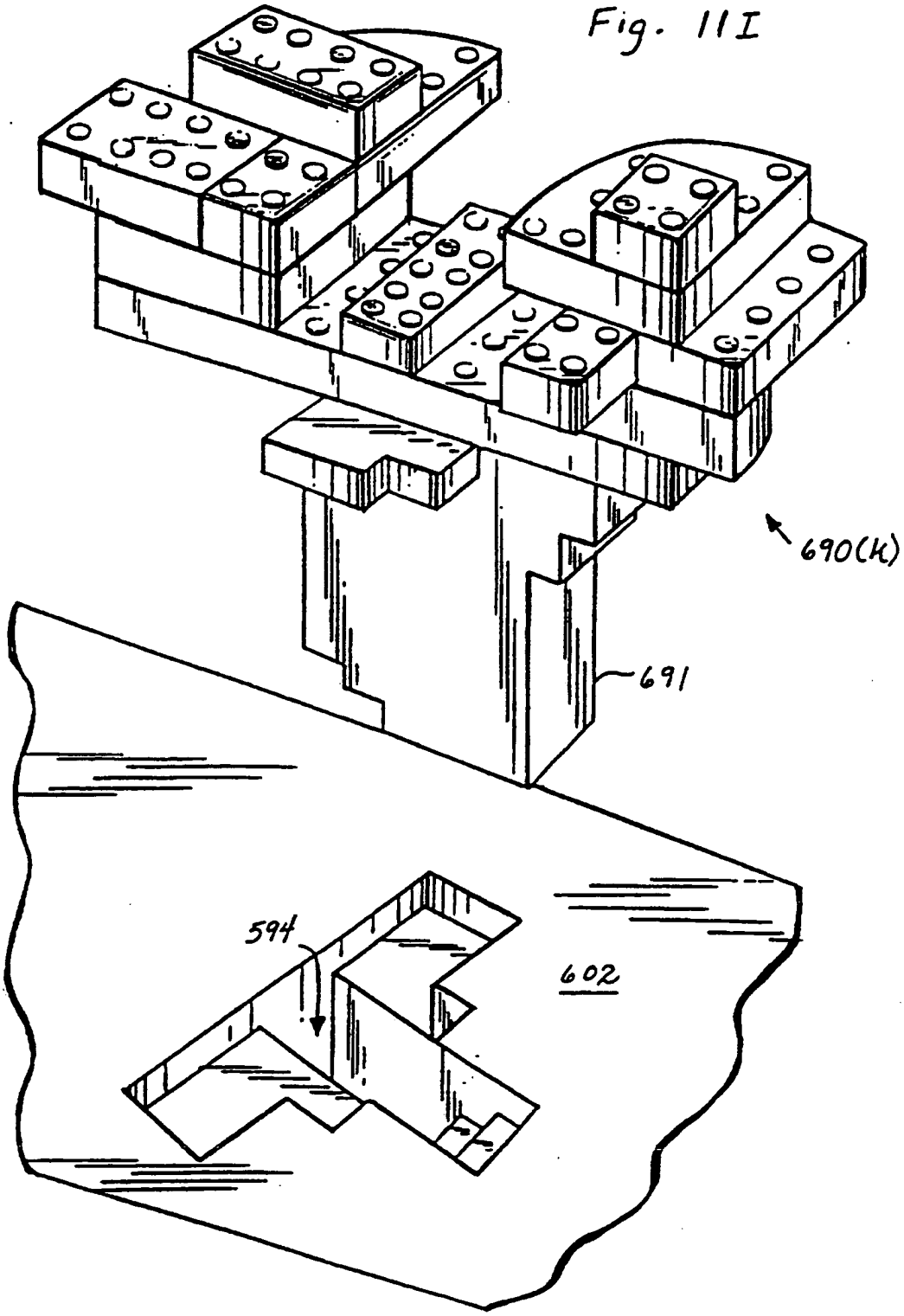


Fig. 11H.
DATA STRUCTURES

Fig. 11I



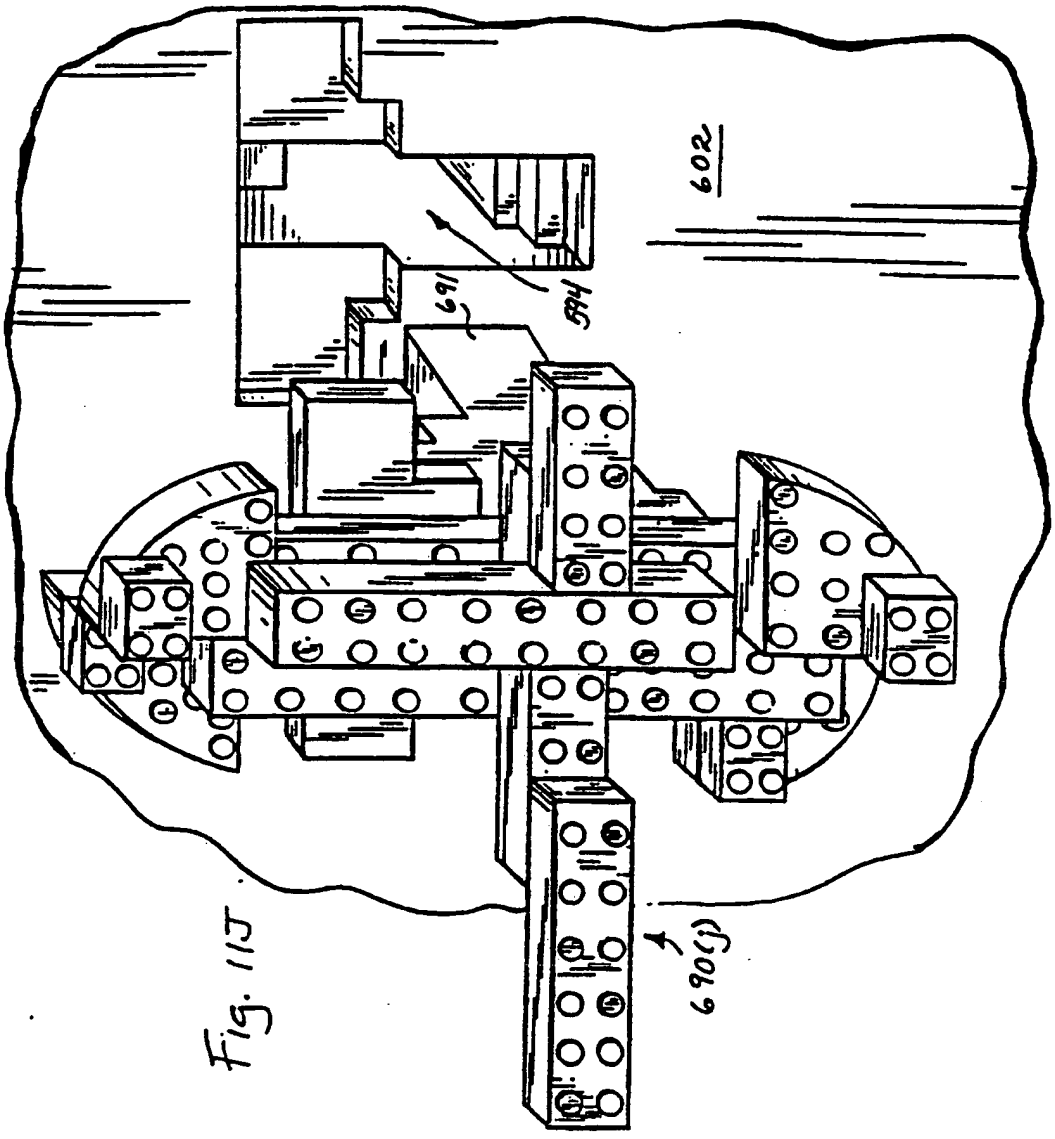


Fig. 11J

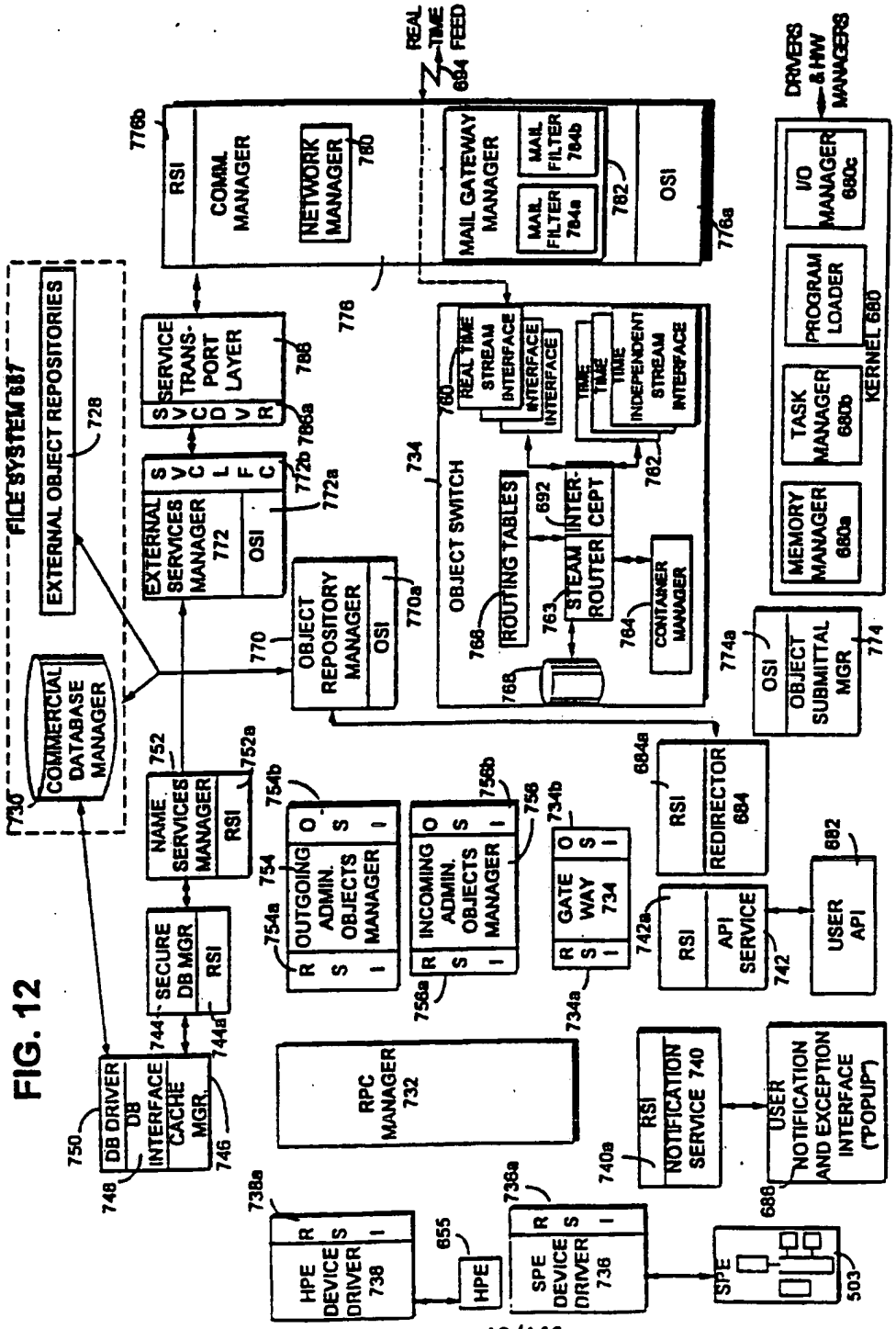

FILE SYSTEM 617
EXTERNAL OBJECT REPOSITORIES
728
COMMERCIAL DATABASE MANAGER
730
752
NAME SERVICES MANAGER
RSI
752a
754b
OUTGOING ADMIN. OBJECTS MANAGER
754
754a
INCOMING ADMIN. OBJECTS MANAGER
756
758b
758a
GATE WAY 734
734b
734a
SECURE DB MGR
RSI
744
744a
DB DRIVER
DB INTERFACE
CACHE MGR
746
748
750
RPC MANAGER 732
HPE DEVICE DRIVER 738
HPE
655
738a
SPE DEVICE DRIVER 738
SPE
503
686
USER NOTIFICATION AND EXCEPTION INTERFACE ("POPUP")
RSI NOTIFICATION SERVICE 740
740a
RSI REDIRECTOR 684
684a
RSI API SERVICE
742
742a
USER API
682
OSI OBJECT SUBMITTAL MGR
774
774a
EXTERNAL SERVICES MANAGER 772
OSI
772
772a
772b
SERVICE TRANS-PORT LAYER
SVCD
VR
786
786a
OBJECT REPOSITORY MANAGER
OSI
770
770a
OBJECT SWITCH
734
ROUTING TABLES
768
STEAM ROUTER
763
INTER-CEPT
692
CONTAINER MANAGER
764
762
REAL TIME STREAM INTERFACE
TIME INDEPENDENT STREAM INTERFACE
780
COMM MANAGER
RSI
776b
NETWORK MANAGER
780
MAIL GATEWAY MANAGER
MAIL FILTER 784a
MAIL FILTER 784b
782
OSI
776a
776
REAL TIME FEED
694
DRIVERS & HW MANAGERS
KERNEL 680
MEMORY MANAGER 680a
TASK MANAGER 680b
PROGRAM LOADER
I/O MANAGER 680c

FIG. 12

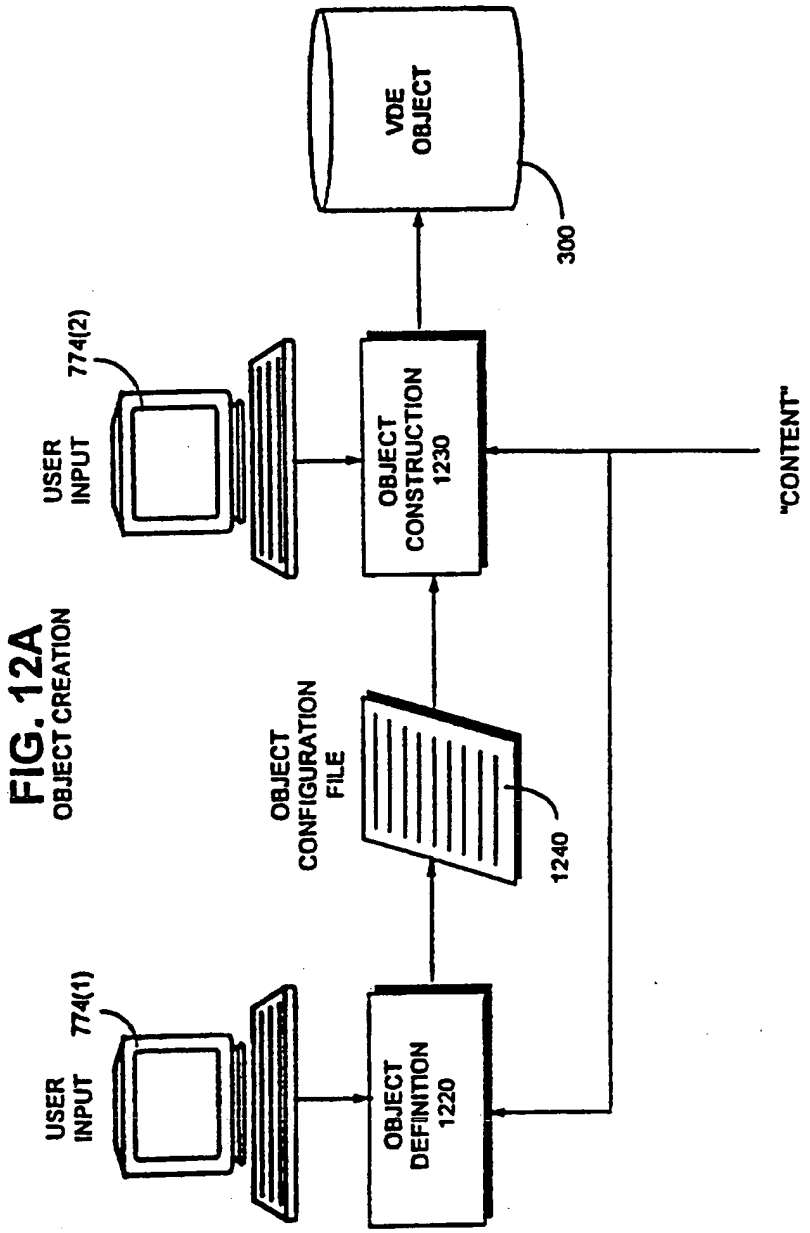


FIG. 12A
OBJECT CREATION

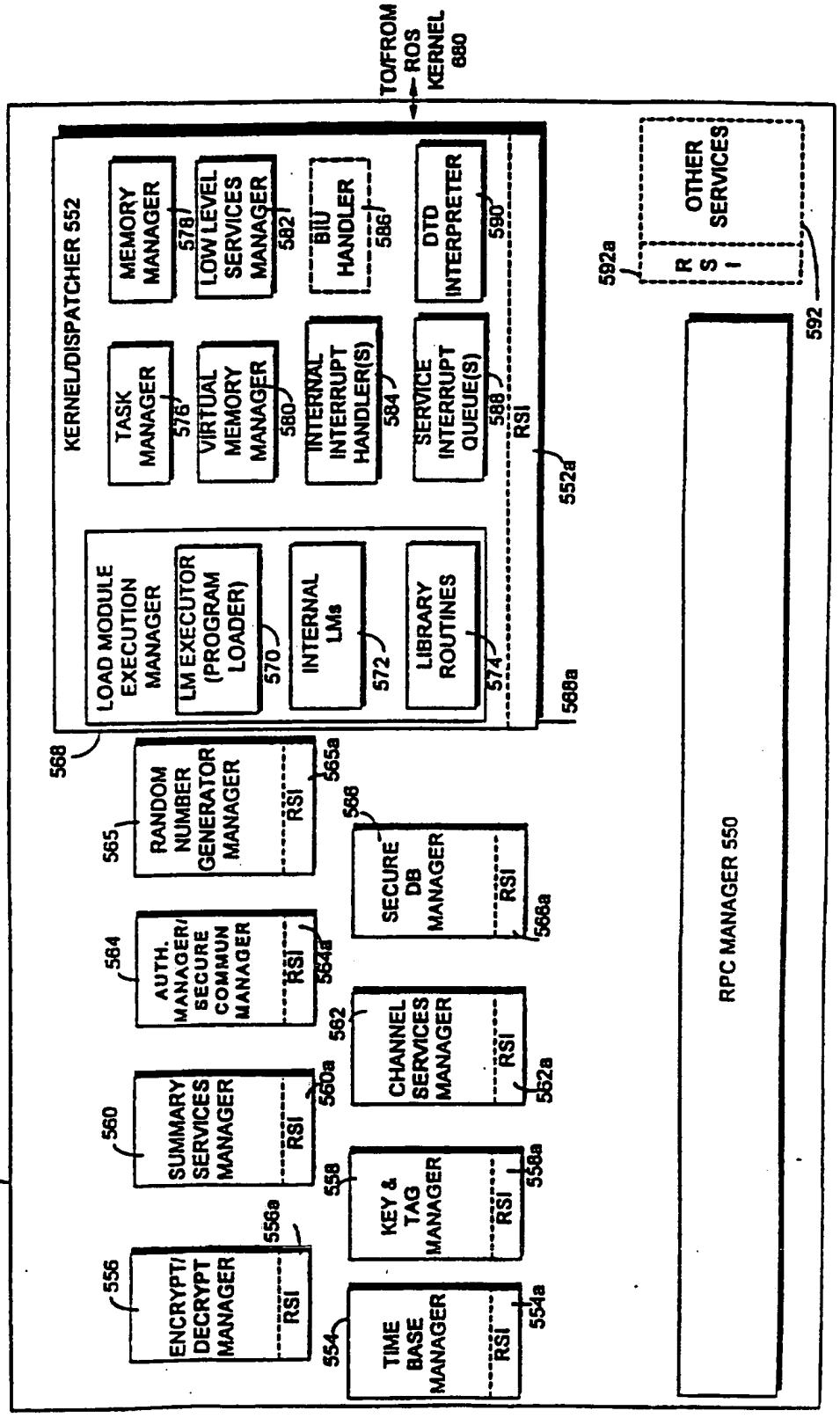

TO/FROM ROS KERNEL 680
PROTECTED PROCESSING ENVIRONMENT 650
503, 655
KERNEL/DISPATCHER 552
MEMORY MANAGER 578
LOW LEVEL SERVICES MANAGER 582
BIU HANDLER 586
DTD INTERPRETER 590
TASK MANAGER 576
VIRTUAL MEMORY MANAGER 580
INTERNAL INTERRUPT HANDLER(S) 584
SERVICE INTERRUPT QUEUE(S) 588
RSI
552a
LOAD MODULE EXECUTION MANAGER
LM EXECUTOR (PROGRAM LOADER) 570
INTERNAL LMs 572
LIBRARY ROUTINES 574
588a
568
RANDOM NUMBER GENERATOR MANAGER 565
RSI 565a
SECURE DB MANAGER 566
RSI 566a
AUTH. MANAGER/ SECURE COMMUN MANAGER 564
RSI 564a
CHANNEL SERVICES MANAGER 562
RSI 562a
SUMMARY SERVICES MANAGER 560
RSI 560a
KEY & TAG MANAGER 558
RSI 558a
ENCRYPT/ DECRYPT MANAGER 556
RSI 556a
TIME BASE MANAGER 554
RSI 554a
RPC MANAGER 550
592
592a
R S I
OTHER SERVICES

FIG. 13

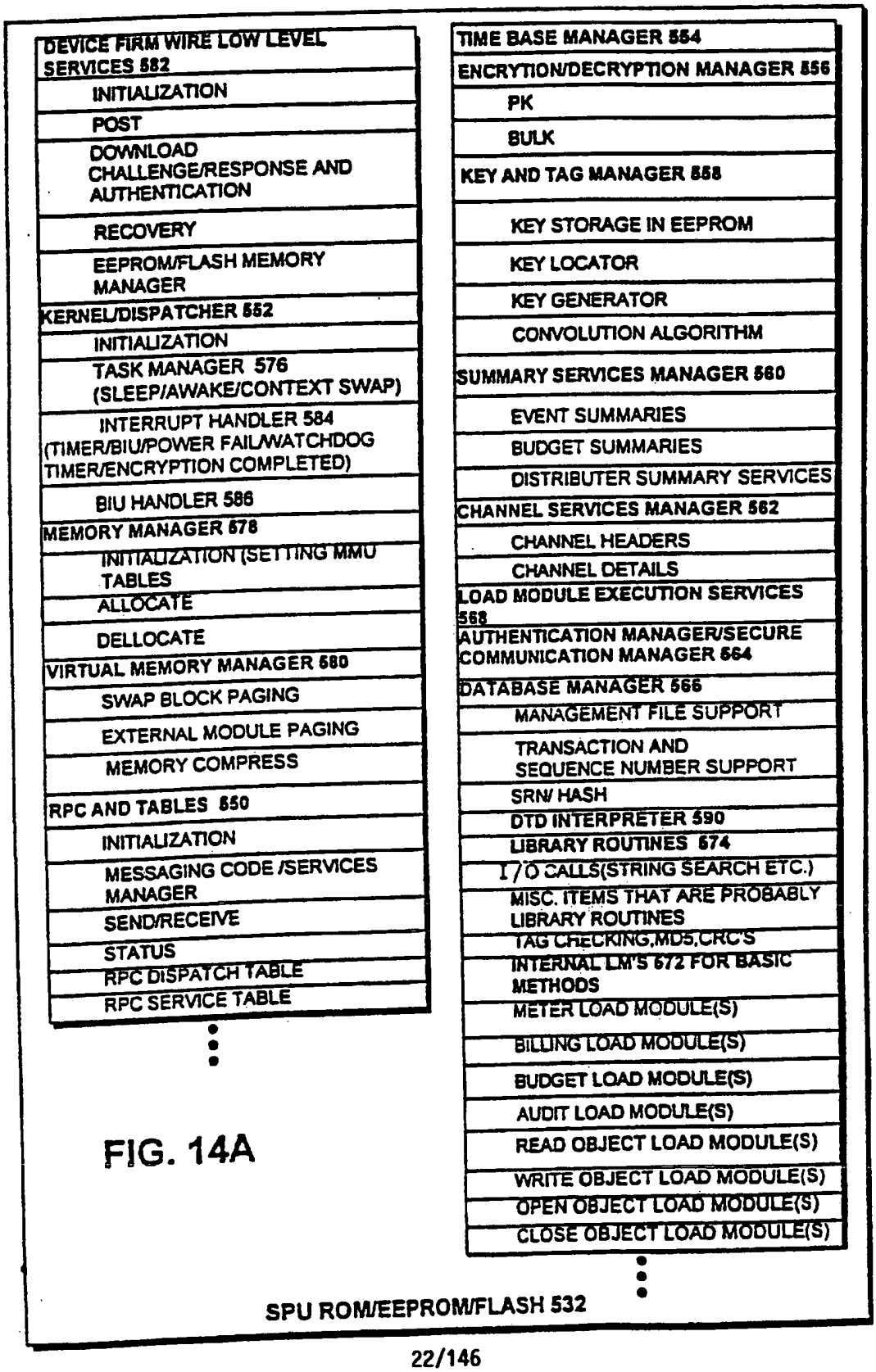

DEVICE FIRM WIRE LOW LEVEL SERVICES 582
INITIALIZATION
POST
DOWNLOAD CHALLENGE/RESPONSE AND AUTHENTICATION
RECOVERY
EEPROM/FLASH MEMORY MANAGER
KERNEL/DISPATCHER 552
INITIALIZATION
TASK MANAGER 576 (SLEEP/AWAKE/CONTEXT SWAP)
INTERRUPT HANDLER 584 (TIMER/BIU/POWER FAIL/WATCHDOG TIMER/ENCRYPTION COMPLETED)
BIU HANDLER 586
MEMORY MANAGER 578
INITIALIZATION (SETTING MMU TABLES
ALLOCATE
DELLOCATE
VIRTUAL MEMORY MANAGER 580
SWAP BLOCK PAGING
EXTERNAL MODULE PAGING
MEMORY COMPRESS
RPC AND TABLES 550
INITIALIZATION
MESSAGING CODE /SERVICES MANAGER
SEND/RECEIVE
STATUS
RPC DISPATCH TABLE
RPC SERVICE TABLE
TIME BASE MANAGER 554
ENCRYTION/DECRYPTION MANAGER 556
PK
BULK
KEY AND TAG MANAGER 558
KEY STORAGE IN EEPROM
KEY LOCATOR
KEY GENERATOR
CONVOLUTION ALGORITHM
SUMMARY SERVICES MANAGER 560
EVENT SUMMARIES
BUDGET SUMMARIES
DISTRIBUTER SUMMARY SERVICES
CHANNEL SERVICES MANAGER 562
CHANNEL HEADERS
CHANNEL DETAILS
LOAD MODULE EXECUTION SERVICES 568
AUTHENTICATION MANAGER/SECURE COMMUNICATION MANAGER 564
DATABASE MANAGER 566
MANAGEMENT FILE SUPPORT
TRANSACTION AND SEQUENCE NUMBER SUPPORT
SRN/ HASH
DTD INTERPRETER 590
LIBRARY ROUTINES 574
I/O CALLS(STRING SEARCH ETC.)
MISC. ITEMS THAT ARE PROBABLY LIBRARY ROUTINES
TAG CHECKING,MD5,CRC'S
INTERNAL LM'S 572 FOR BASIC METHODS
METER LOAD MODULE(S)
BILLING LOAD MODULE(S)
BUDGET LOAD MODULE(S)
AUDIT LOAD MODULE(S)
READ OBJECT LOAD MODULE(S)
WRITE OBJECT LOAD MODULE(S)
OPEN OBJECT LOAD MODULE(S)
CLOSE OBJECT LOAD MODULE(S)
SPU ROM/EEPROM/FLASH 532

FIG. 14A

FIG. 14B

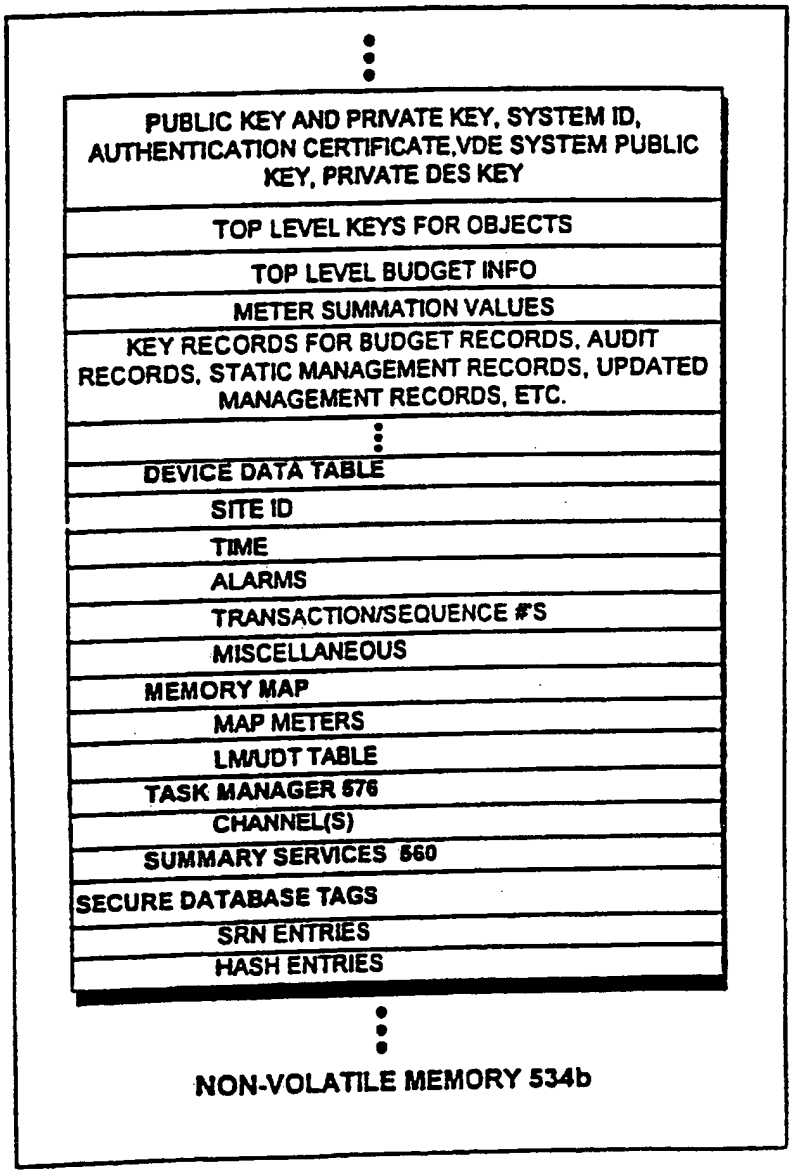
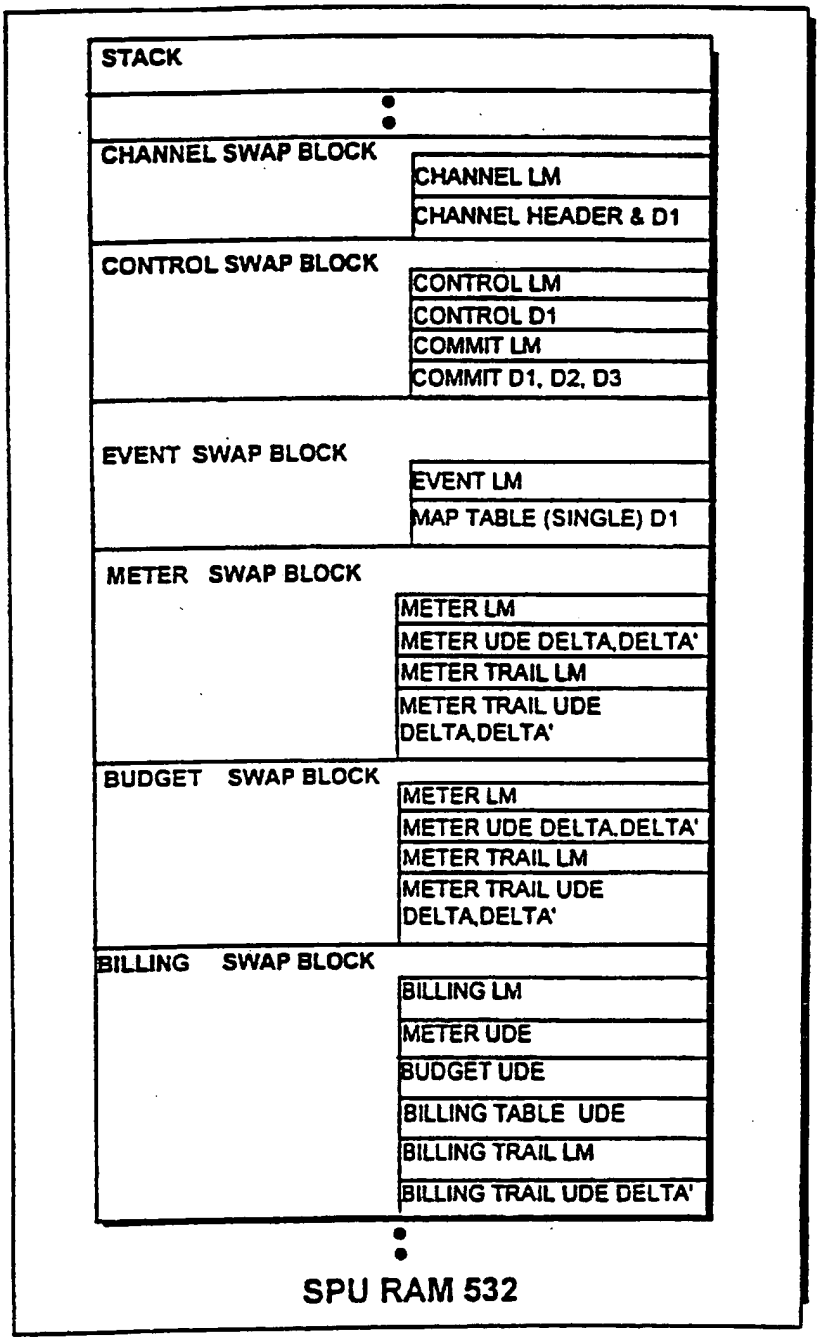

PUBLIC KEY AND PRIVATE KEY, SYSTEM ID, AUTHENTICATION CERTIFICATE,VDE SYSTEM PUBLIC KEY, PRIVATE DES KEY
TOP LEVEL KEYS FOR OBJECTS
TOP LEVEL BUDGET INFO
METER SUMMATION VALUES
KEY RECORDS FOR BUDGET RECORDS, AUDIT RECORDS, STATIC MANAGEMENT RECORDS, UPDATED MANAGEMENT RECORDS, ETC.
DEVICE DATA TABLE
SITE ID
TIME
ALARMS
TRANSACTION/SEQUENCE #'S
MISCELLANEOUS
MEMORY MAP
MAP METERS
LM/UDT TABLE
TASK MANAGER 576
CHANNEL(S)
SUMMARY SERVICES 560
SECURE DATABASE TAGS
SRN ENTRIES
HASH ENTRIES
NON-VOLATILE MEMORY 534b

FIG. 14C


STACK
CHANNEL SWAP BLOCK
CHANNEL LM
CHANNEL HEADER & D1
CONTROL SWAP BLOCK
CONTROL LM
CONTROL D1
COMMIT LM
COMMIT D1, D2, D3
EVENT SWAP BLOCK
EVENT LM
MAP TABLE (SINGLE) D1
METER SWAP BLOCK
METER LM
METER UDE DELTA,DELTA'
METER TRAIL LM
METER TRAIL UDE DELTA,DELTA'
BUDGET SWAP BLOCK
METER LM
METER UDE DELTA,DELTA'
METER TRAIL LM
METER TRAIL UDE DELTA,DELTA'
BILLING SWAP BLOCK
BILLING LM
METER UDE
BUDGET UDE
BILLING TABLE UDE
BILLING TRAIL LM
BILLING TRAIL UDE DELTA'
SPU RAM 532

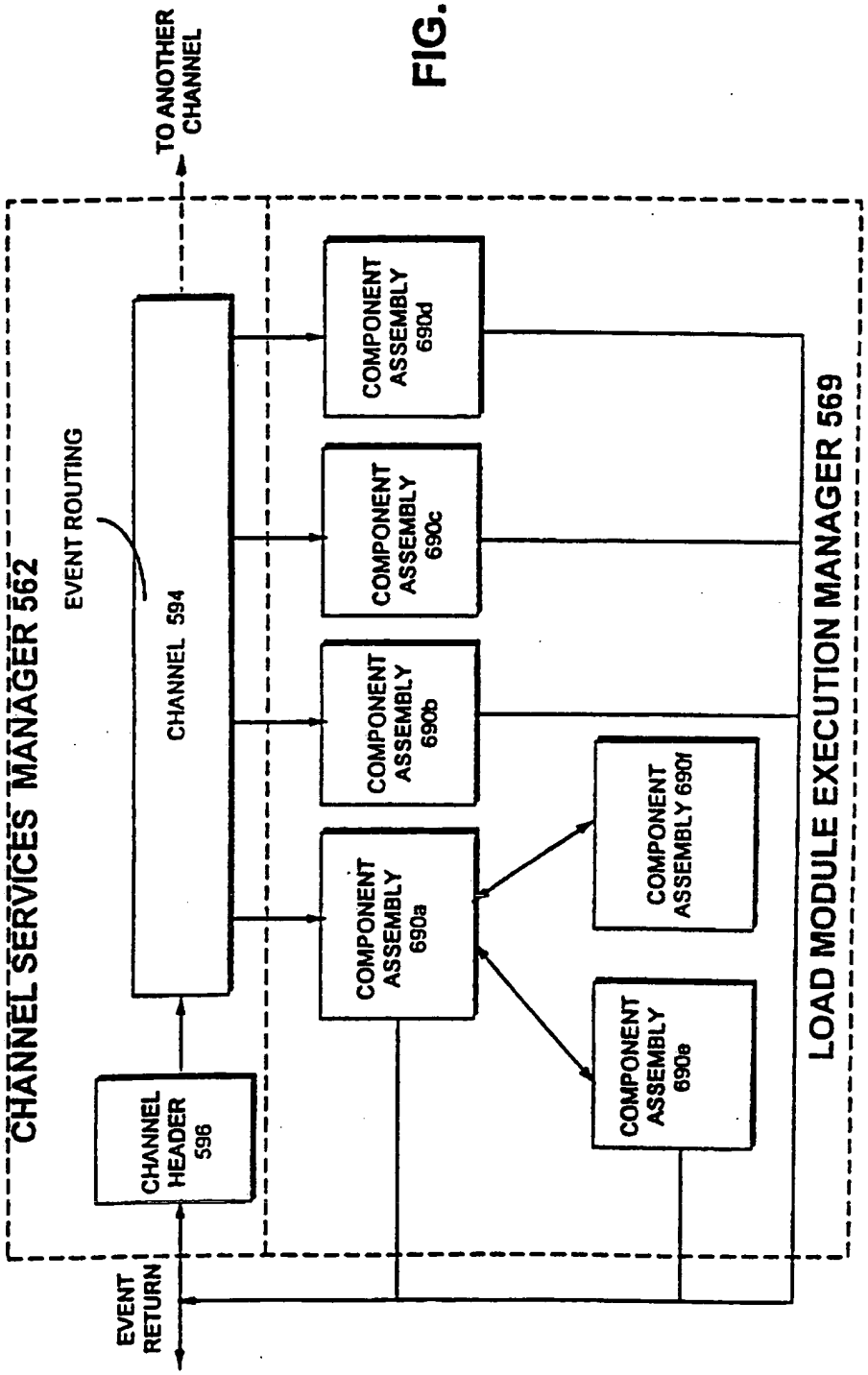

TO ANOTHER CHANNEL
CHANNEL SERVICES MANAGER 562
EVENT ROUTING
CHANNEL 594
COMPONENT ASSEMBLY 690d
COMPONENT ASSEMBLY 690c
COMPONENT ASSEMBLY 690b
COMPONENT ASSEMBLY 690a
COMPONENT ASSEMBLY 690f
COMPONENT ASSEMBLY 690e
CHANNEL HEADER 596
LOAD MODULE EXECUTION MANAGER 569
EVENT RETURN

FIG. 15

FIG. 15A

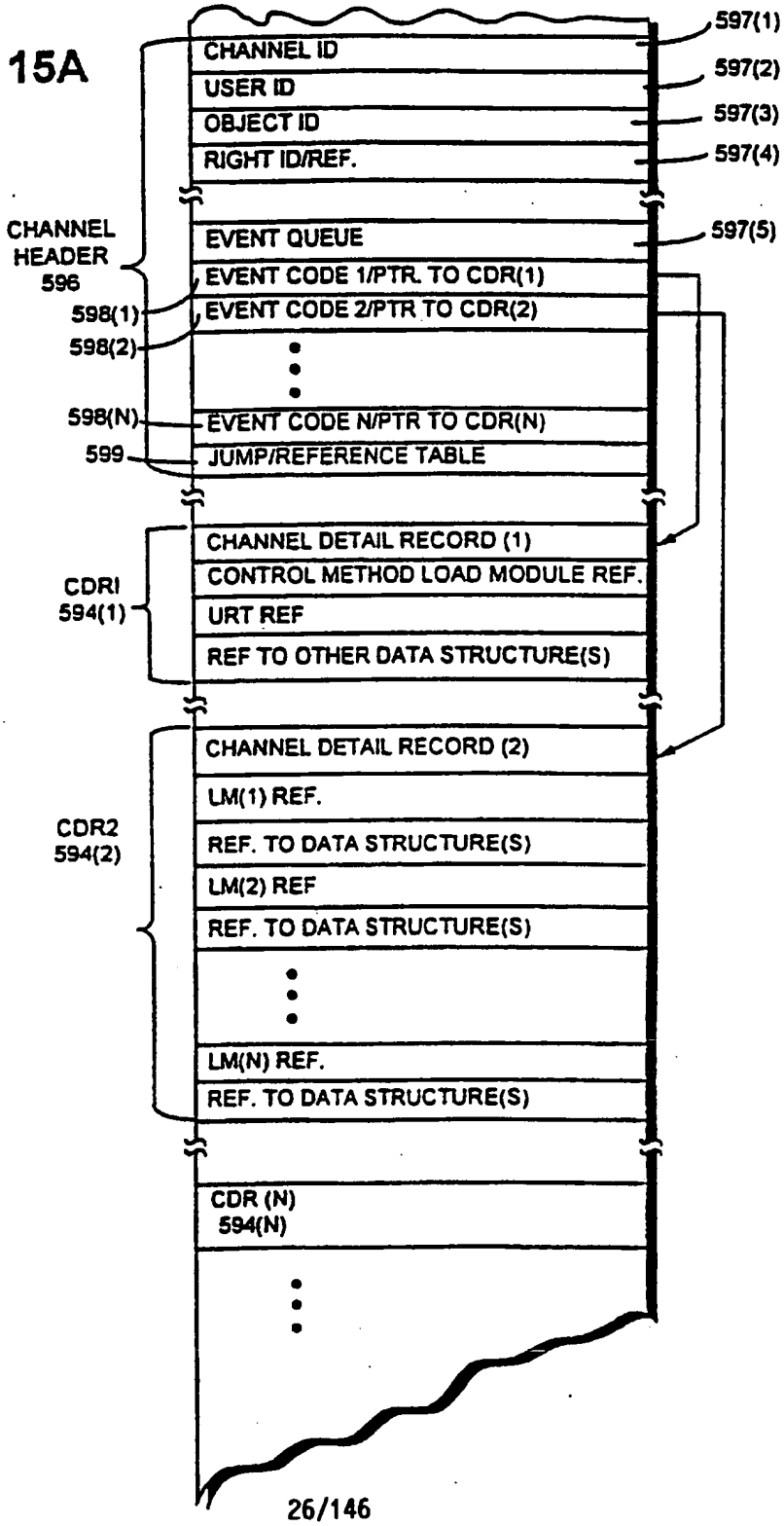

597(1)
CHANNEL ID
597(2)
USER ID
597(3)
OBJECT ID
597(4)
RIGHT ID/REF.
CHANNEL HEADER 596
597(5)
EVENT QUEUE
EVENT CODE 1/PTR. TO CDR(1)
598(1)
EVENT CODE 2/PTR TO CDR(2)
598(2)
598(N)
EVENT CODE N/PTR TO CDR(N)
599
JUMP/REFERENCE TABLE
CDRI 594(1)
CHANNEL DETAIL RECORD (1)
CONTROL METHOD LOAD MODULE REF.
URT REF
REF TO OTHER DATA STRUCTURE(S)
CDR2 594(2)
CHANNEL DETAIL RECORD (2)
LM(1) REF.
REF. TO DATA STRUCTURE(S)
LM(2) REF
REF. TO DATA STRUCTURE(S)
LM(N) REF.
REF. TO DATA STRUCTURE(S)
CDR (N) 594(N)

FIG. 15B

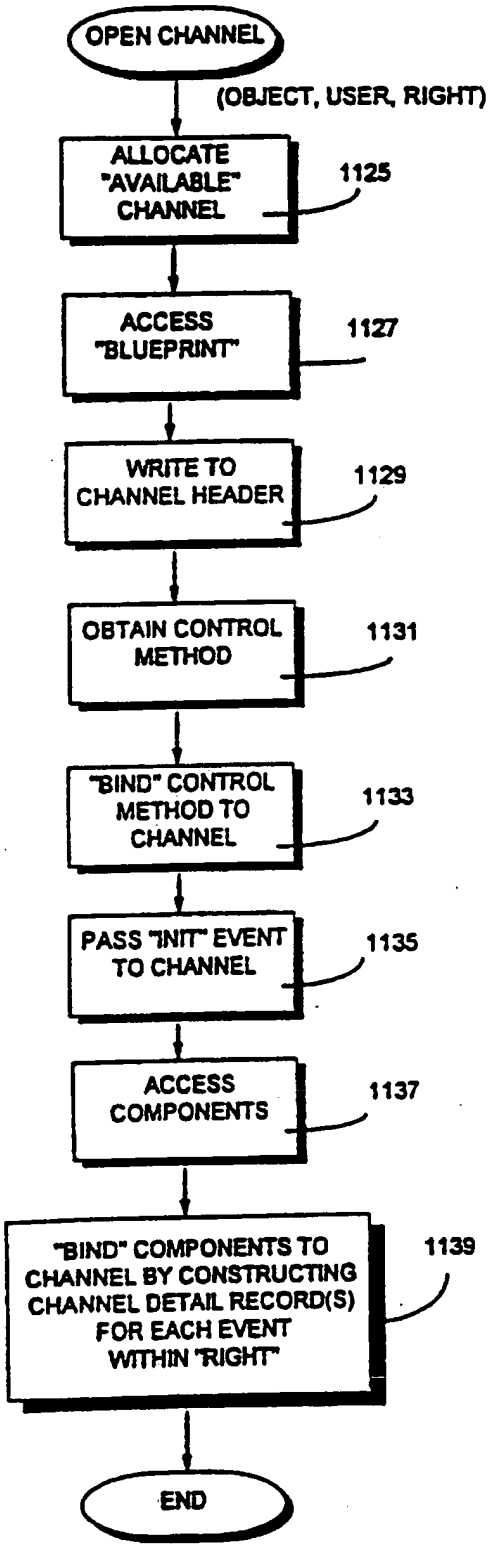
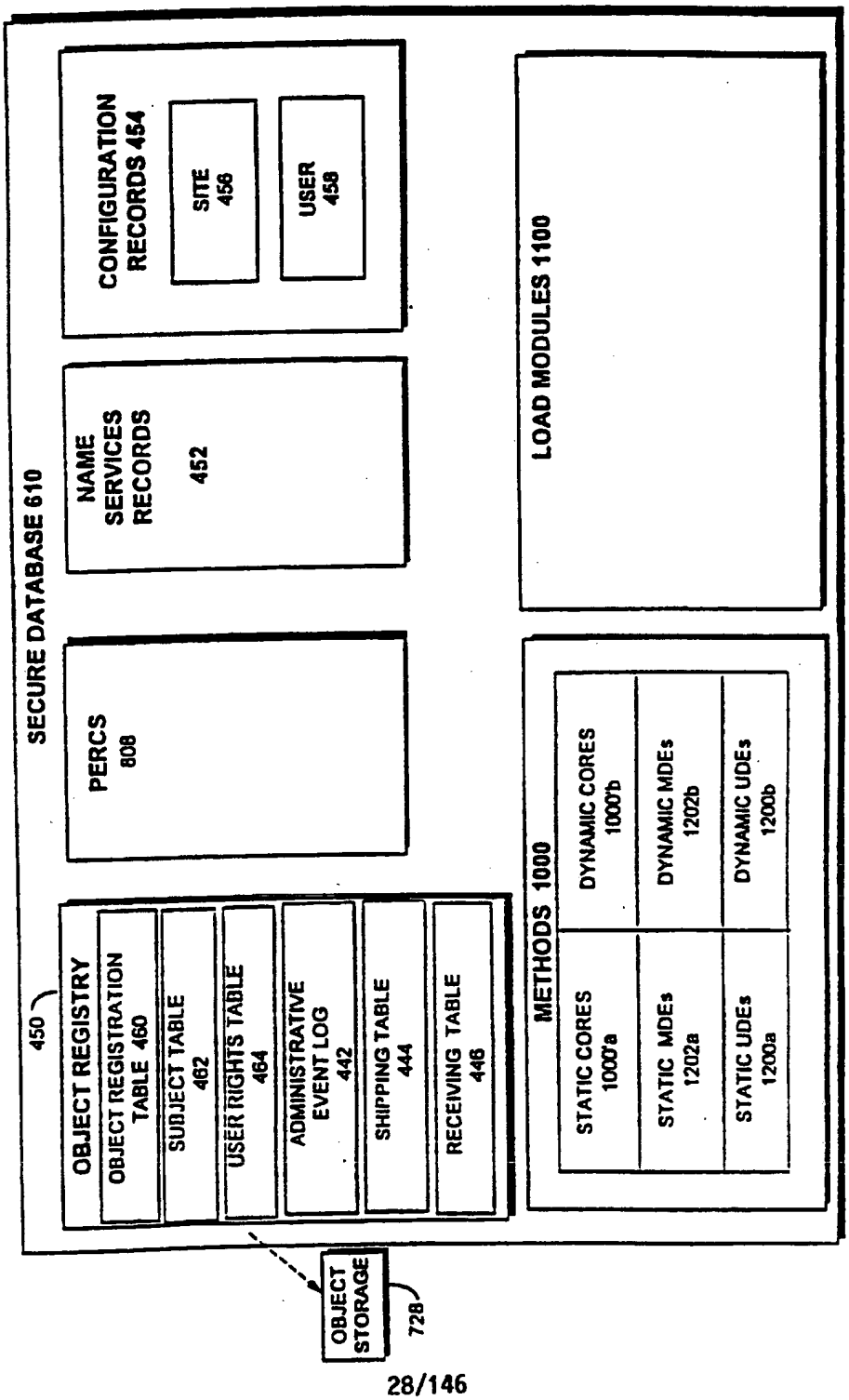

OPEN CHANNEL
(OBJECT, USER, RIGHT)
ALLOCATE "AVAILABLE" CHANNEL
1125
ACCESS "BLUEPRINT"
1127
WRITE TO CHANNEL HEADER
1129
OBTAIN CONTROL METHOD
1131
"BIND" CONTROL METHOD TO CHANNEL
1133
PASS "INIT" EVENT TO CHANNEL
1135
ACCESS COMPONENTS
1137
"BIND" COMPONENTS TO CHANNEL BY CONSTRUCTING CHANNEL DETAIL RECORD(S) FOR EACH EVENT WITHIN "RIGHT"
1139
END

FIG. 16


SECURE DATABASE 610
450
OBJECT REGISTRY
OBJECT REGISTRATION TABLE 460
SUBJECT TABLE 462
USER RIGHTS TABLE 464
ADMINISTRATIVE EVENT LOG 442
SHIPPING TABLE 444
RECEIVING TABLE 446
PERCS 808
NAME SERVICES RECORDS 452
CONFIGURATION RECORDS 454
SITE 456
USER 458
LOAD MODULES 1100
METHODS 1000
STATIC CORES 1000a
STATIC MDEs 1202a
STATIC UDEs 1200a
DYNAMIC CORES 1000b
DYNAMIC MDEs 1202b
DYNAMIC UDEs 1200b
OBJECT STORAGE
728

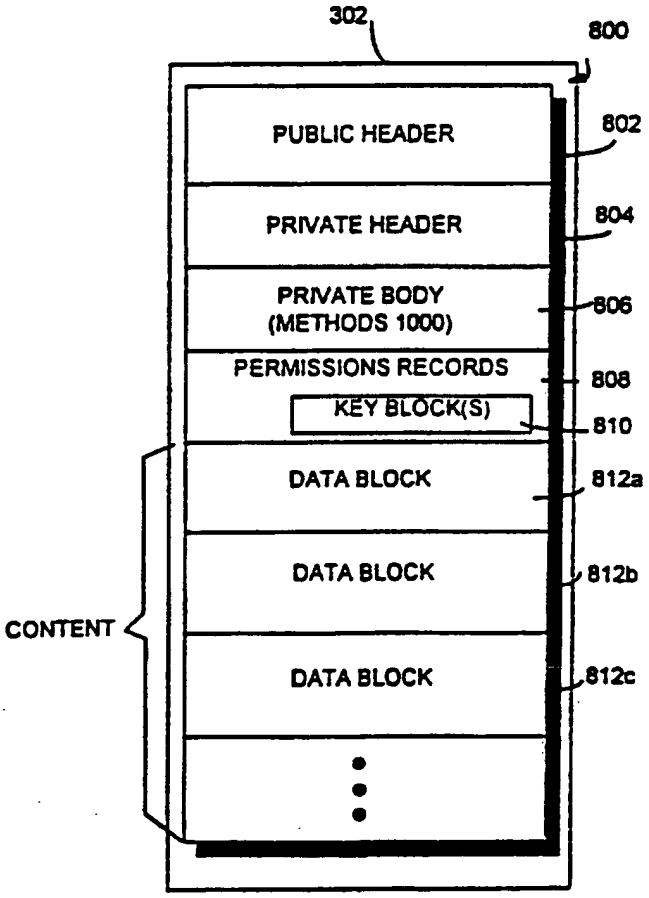
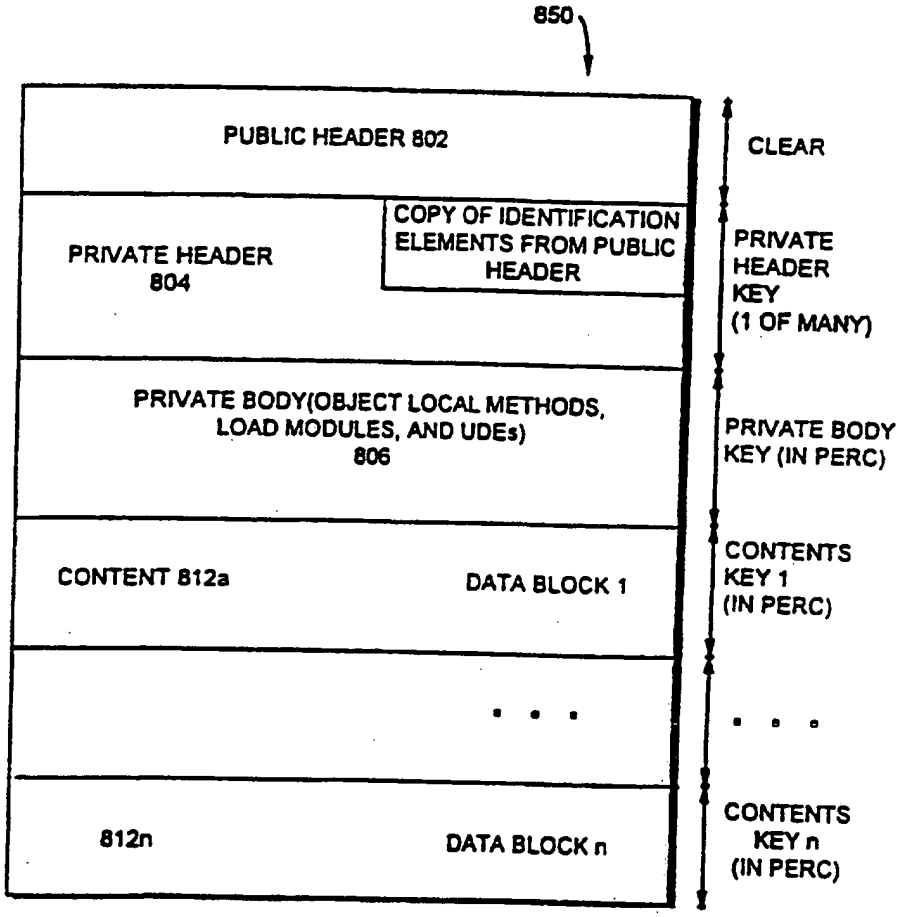
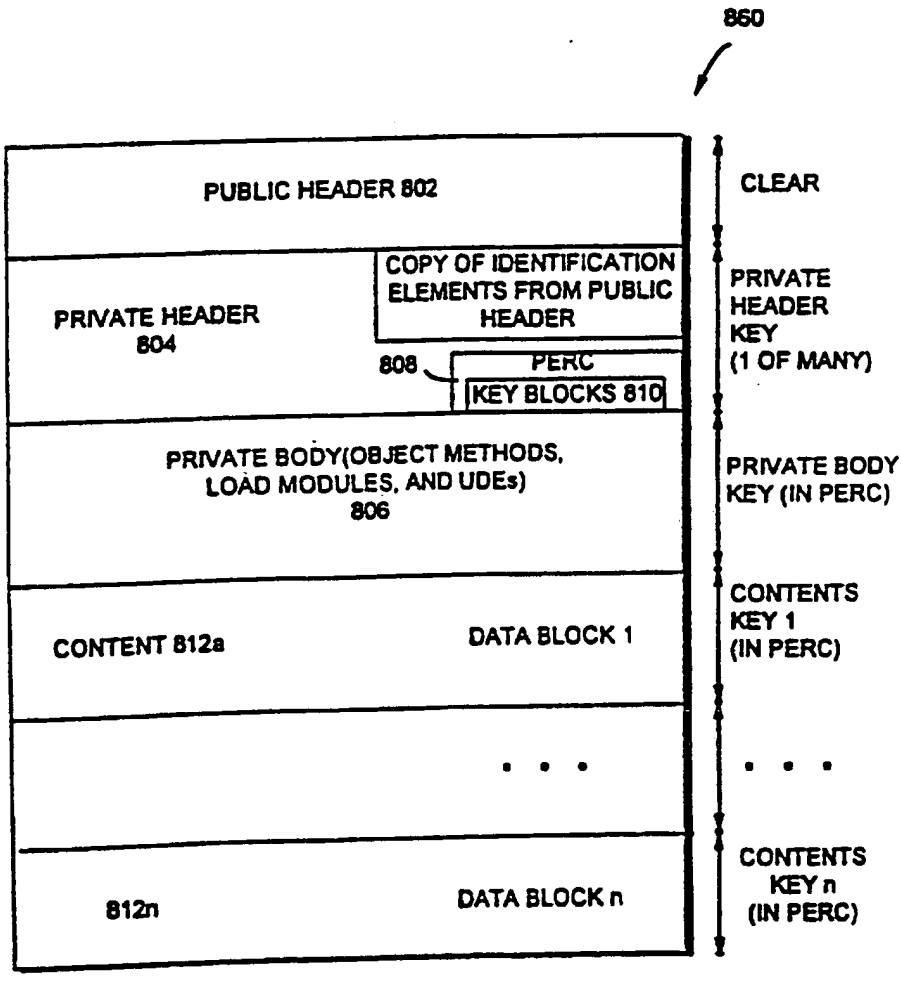

302
800
PUBLIC HEADER
802
PRIVATE HEADER
804
PRIVATE BODY
(METHODS 1000)
806
PERMISSIONS RECORDS
808
KEY BLOCK(S)
810
DATA BLOCK
812a
DATA BLOCK
812b
DATA BLOCK
812c
CONTENT
LOGICAL OBJECT

FIG. 17



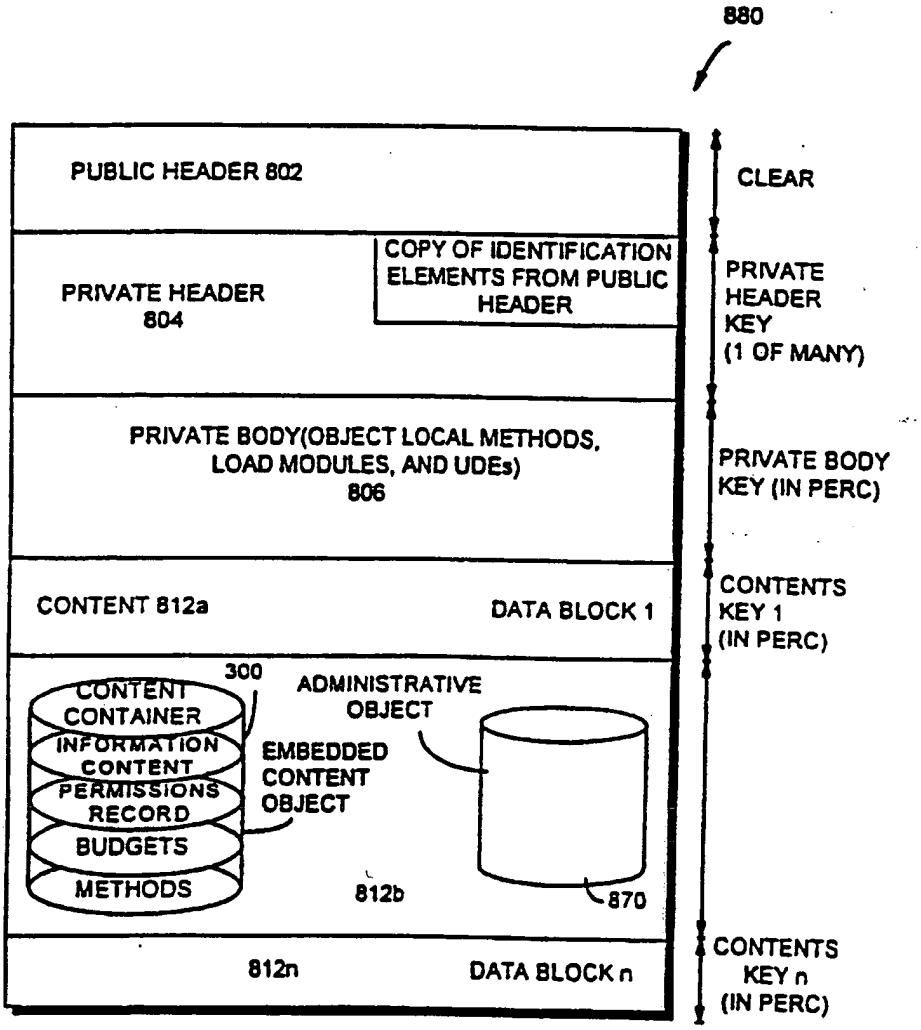
STATIONARY OBJECT

FIG. 18



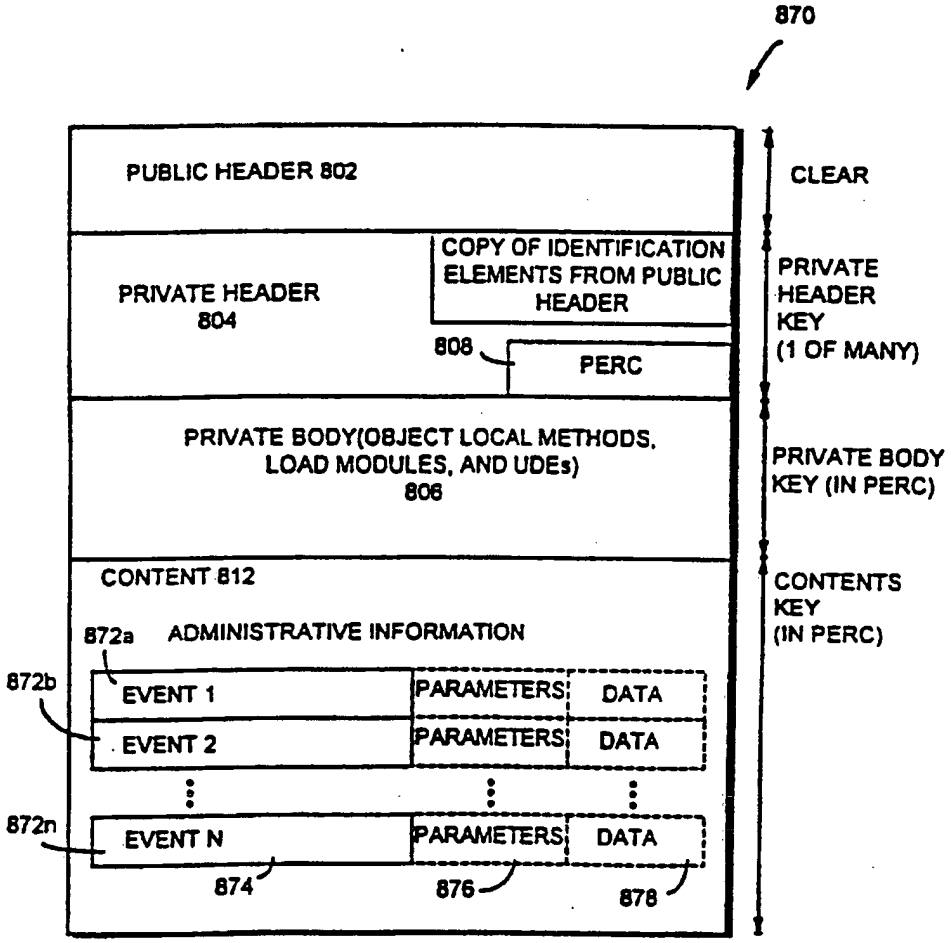
TRAVELING OBJECT

FIG. 19



CONTENT OBJECT

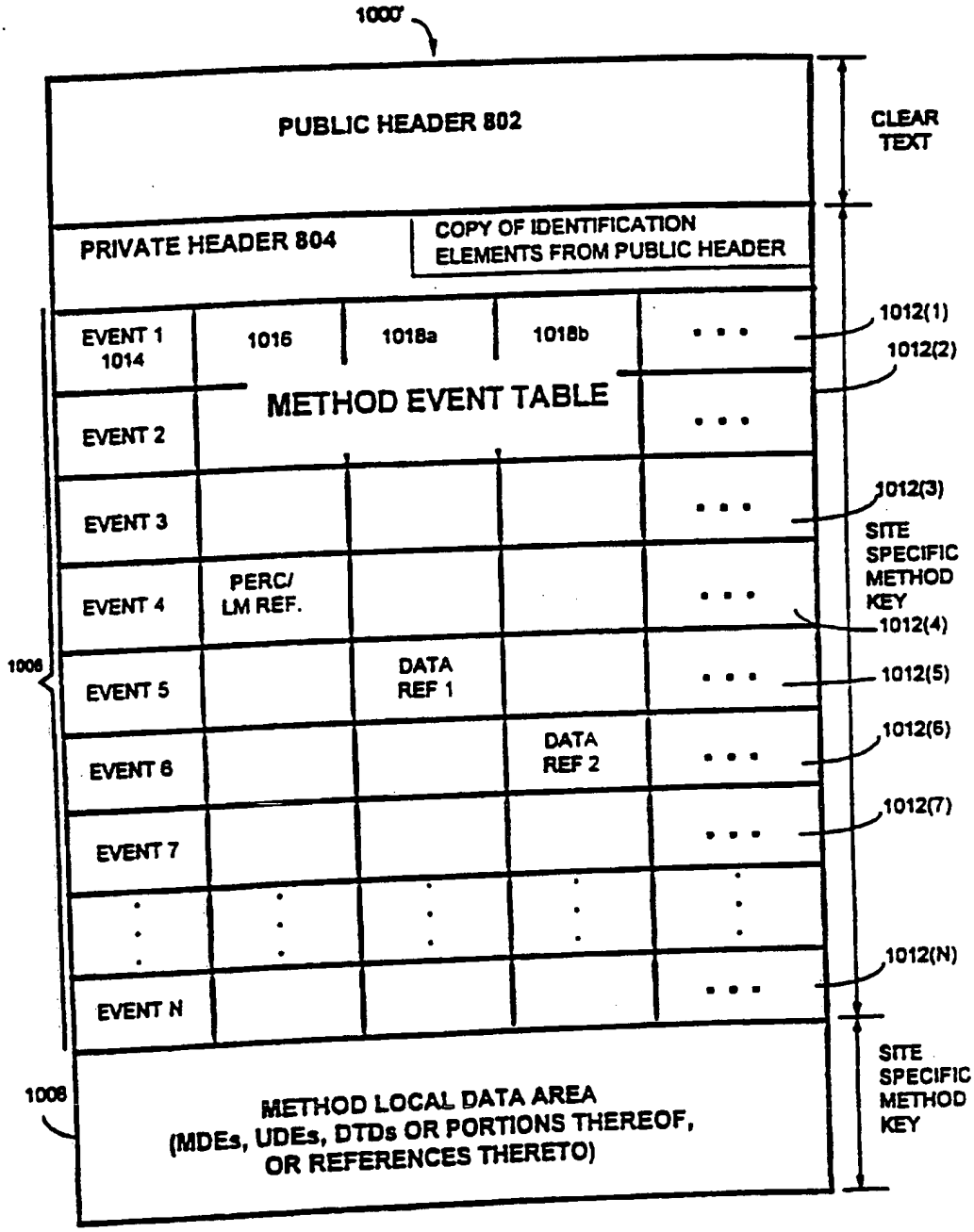
FIG. 20



ADMINISTRATIVE OBJECT

FIG. 21

FIG. 22



METHOD "CORE"

FIG. 23

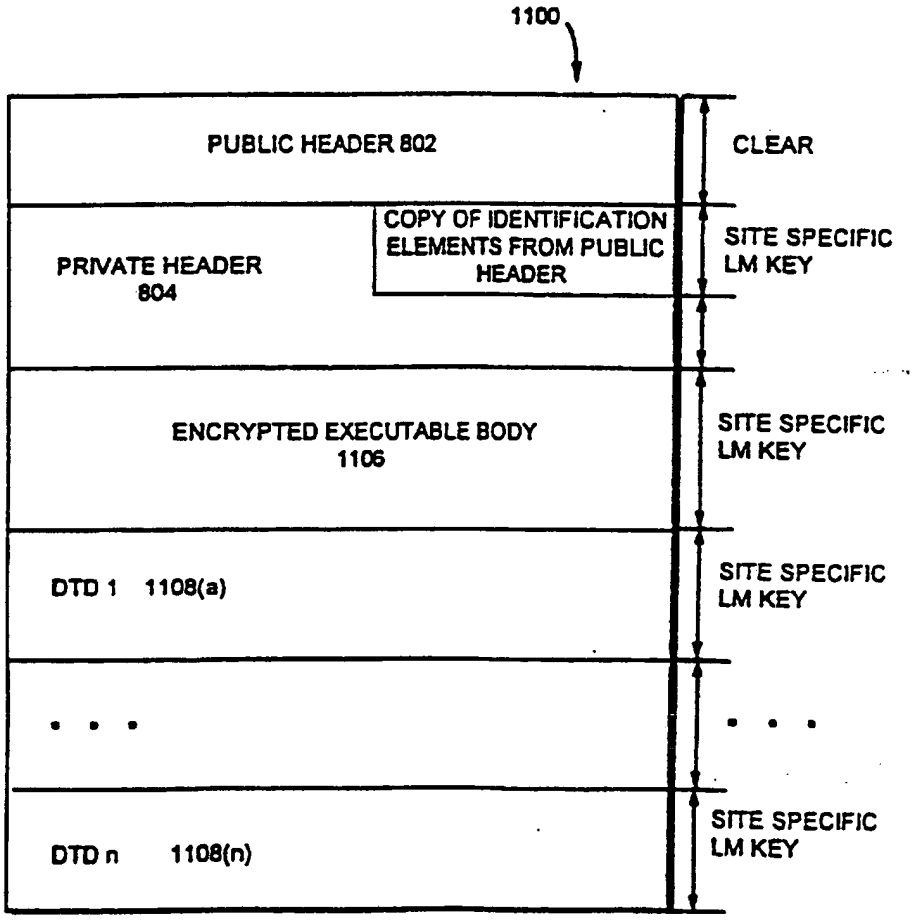
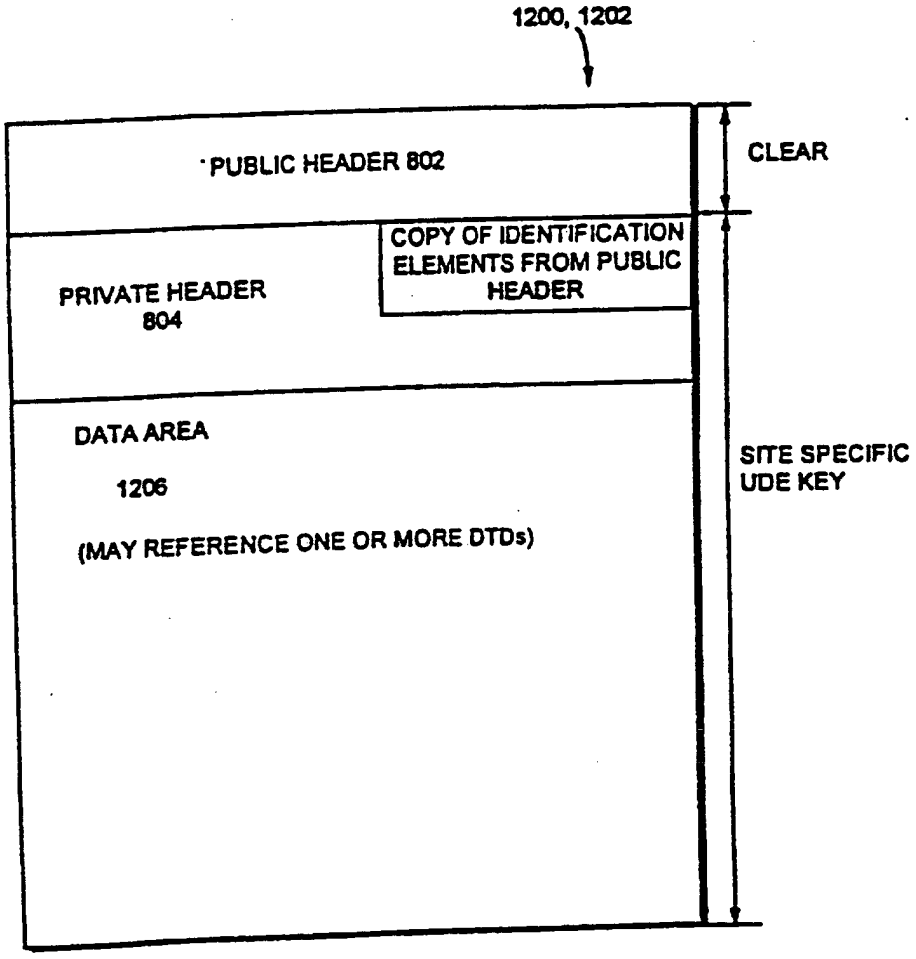

1100
PUBLIC HEADER 802
CLEAR
COPY OF IDENTIFICATION ELEMENTS FROM PUBLIC HEADER
PRIVATE HEADER 804
SITE SPECIFIC LM KEY
ENCRYPTED EXECUTABLE BODY 1106
SITE SPECIFIC LM KEY
DTD 1 1108(a)
SITE SPECIFIC LM KEY
• • •
• • •
DTD n 1108(n)
SITE SPECIFIC LM KEY
LOAD MODULE

FIG. 24



UDE (MDE)

FIG. 25A

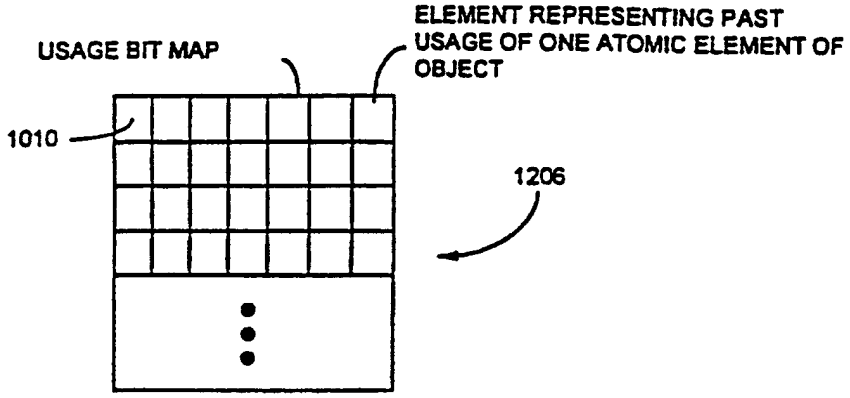


FIG. 25B

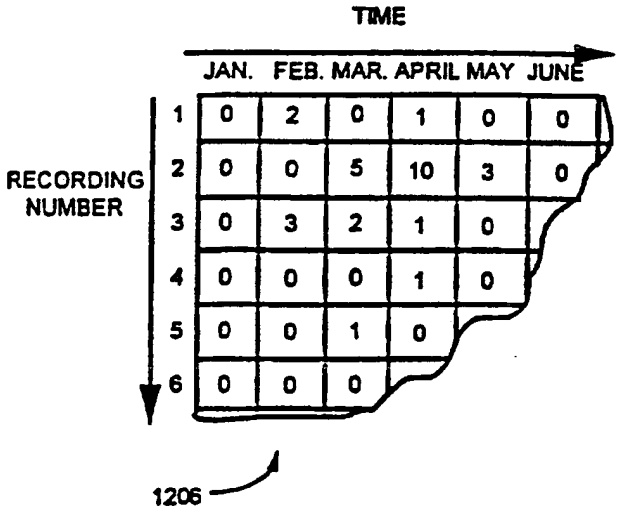


FIG. 25C

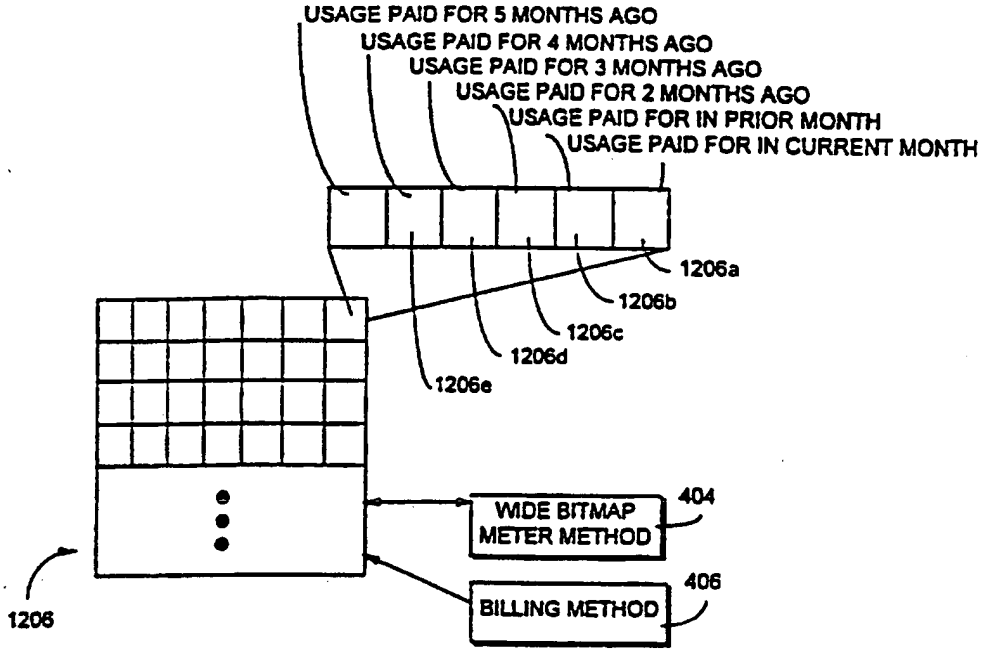

USAGE PAID FOR 5 MONTHS AGO
USAGE PAID FOR 4 MONTHS AGO
USAGE PAID FOR 3 MONTHS AGO
USAGE PAID FOR 2 MONTHS AGO
USAGE PAID FOR IN PRIOR MONTH
USAGE PAID FOR IN CURRENT MONTH
1206a
1206b
1206c
1206d
1206e
WIDE BITMAP METER METHOD
404
BILLING METHOD
406
1206

FIG. 26

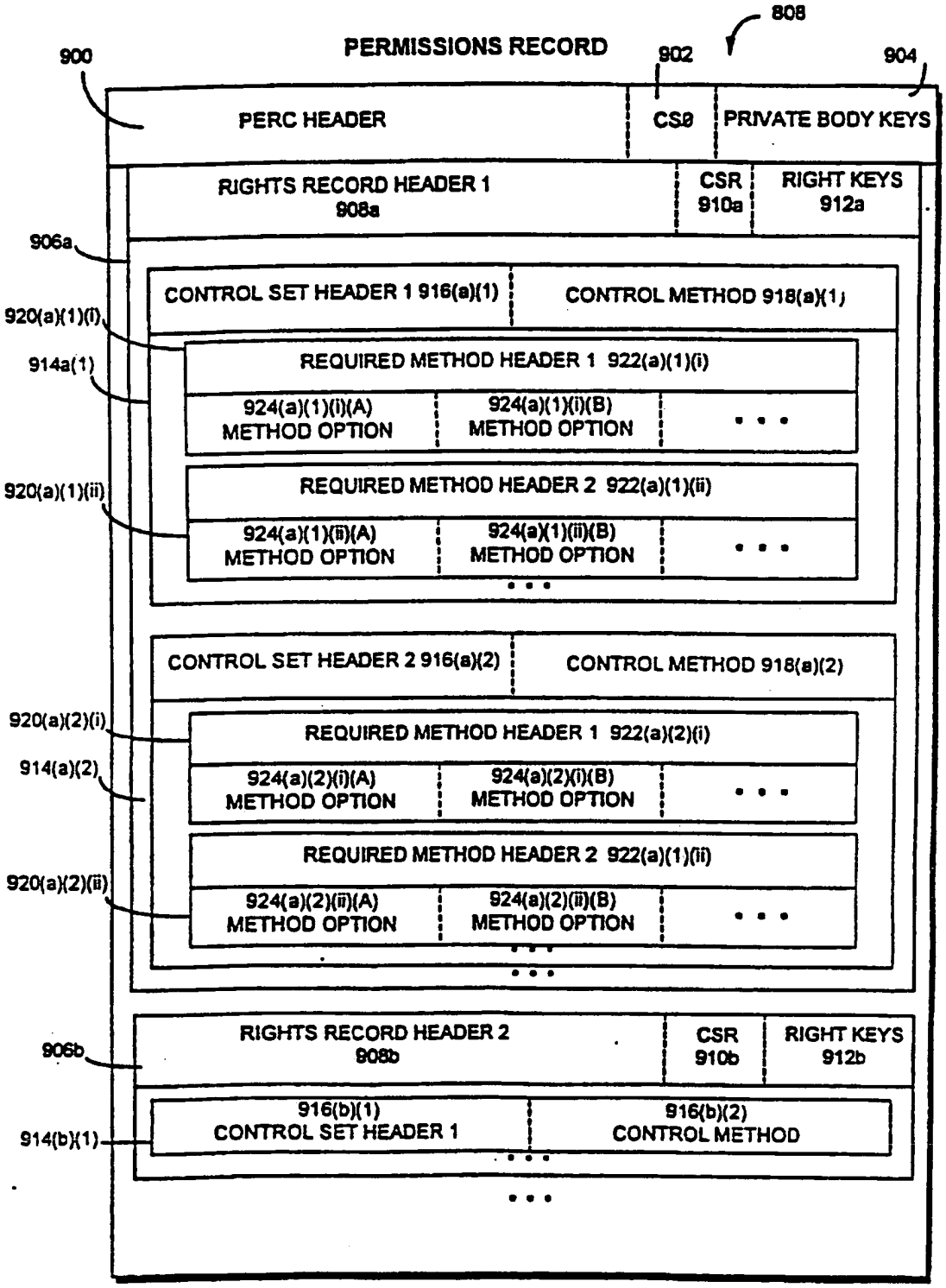
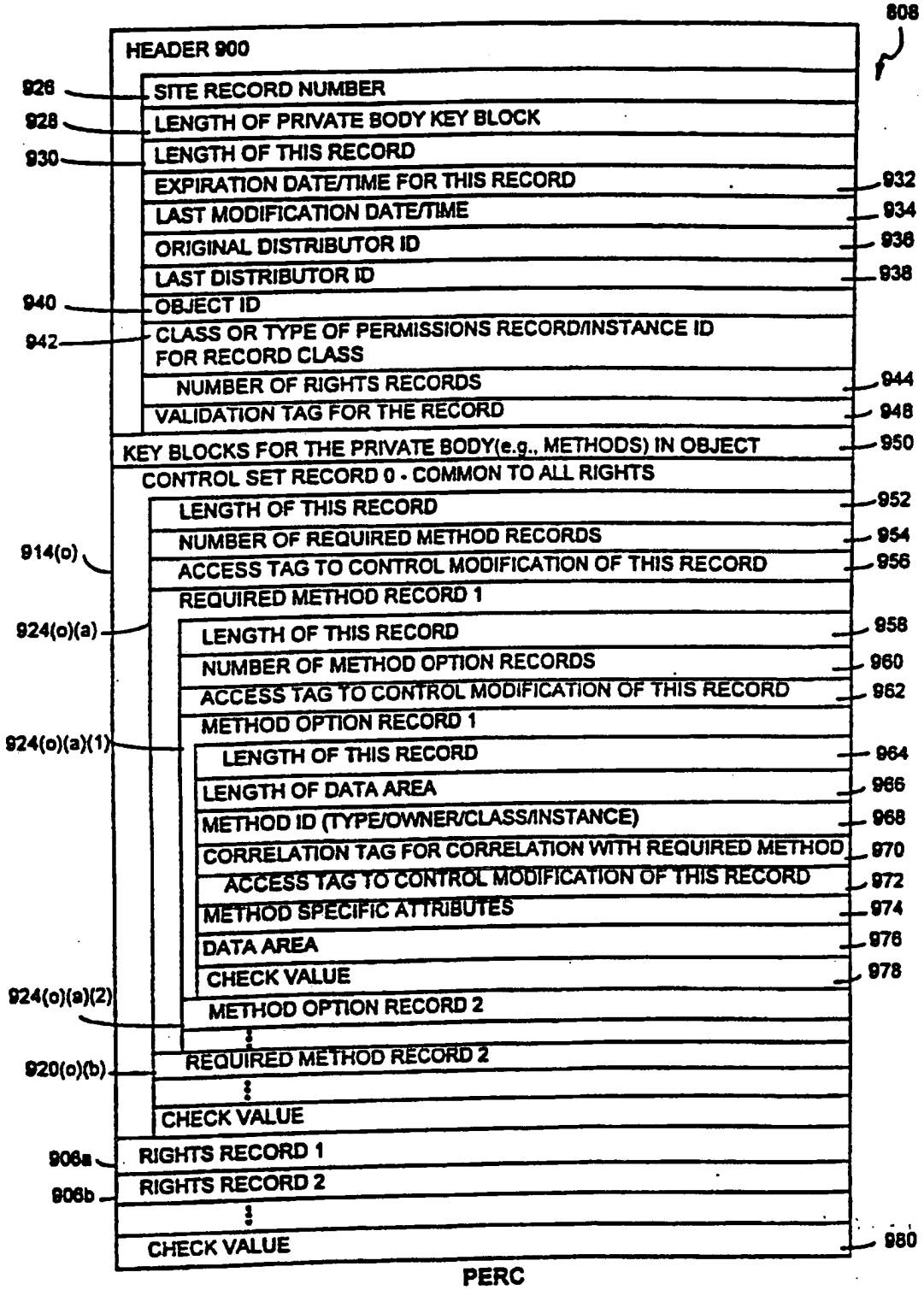
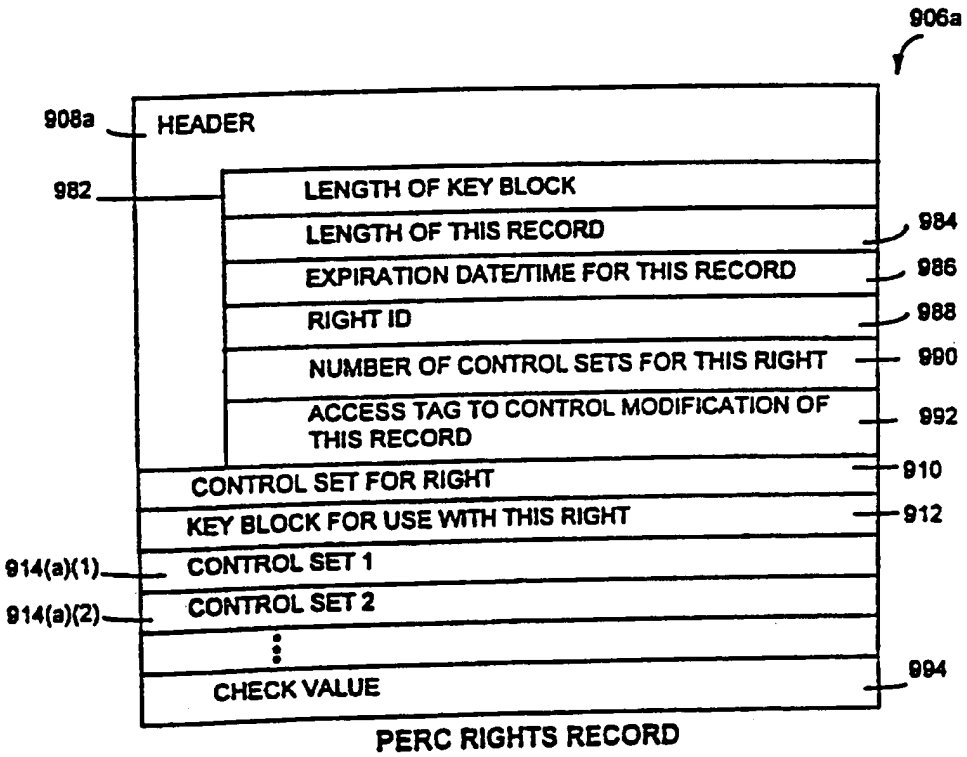

808
PERMISSIONS RECORD
900
902
904
PERC HEADER
CS0
PRIVATE BODY KEYS
RIGHTS RECORD HEADER 1
908a
CSR
910a
RIGHT KEYS
912a
906a
CONTROL SET HEADER 1 916(a)(1)
CONTROL METHOD 918(a)(1)
920(a)(1)(i)
914a(1)
REQUIRED METHOD HEADER 1 922(a)(1)(i)
924(a)(1)(i)(A) METHOD OPTION
924(a)(1)(i)(B) METHOD OPTION
920(a)(1)(ii)
REQUIRED METHOD HEADER 2 922(a)(1)(ii)
924(a)(1)(ii)(A) METHOD OPTION
924(a)(1)(ii)(B) METHOD OPTION
CONTROL SET HEADER 2 916(a)(2)
CONTROL METHOD 918(a)(2)
920(a)(2)(i)
914(a)(2)
REQUIRED METHOD HEADER 1 922(a)(2)(i)
924(a)(2)(i)(A) METHOD OPTION
924(a)(2)(i)(B) METHOD OPTION
920(a)(2)(ii)
REQUIRED METHOD HEADER 2 922(a)(1)(ii)
924(a)(2)(ii)(A) METHOD OPTION
924(a)(2)(ii)(B) METHOD OPTION
RIGHTS RECORD HEADER 2
908b
CSR
910b
RIGHT KEYS
912b
906b
916(b)(1) CONTROL SET HEADER 1
916(b)(2) CONTROL METHOD
914(b)(1)

FIG. 26A


808
HEADER 900
926
SITE RECORD NUMBER
928
LENGTH OF PRIVATE BODY KEY BLOCK
930
LENGTH OF THIS RECORD
EXPIRATION DATE/TIME FOR THIS RECORD
932
LAST MODIFICATION DATE/TIME
934
ORIGINAL DISTRIBUTOR ID
936
LAST DISTRIBUTOR ID
938
940
OBJECT ID
942
CLASS OR TYPE OF PERMISSIONS RECORD/INSTANCE ID FOR RECORD CLASS
NUMBER OF RIGHTS RECORDS
944
VALIDATION TAG FOR THE RECORD
948
KEY BLOCKS FOR THE PRIVATE BODY(e.g., METHODS) IN OBJECT
950
CONTROL SET RECORD 0 - COMMON TO ALL RIGHTS
LENGTH OF THIS RECORD
952
NUMBER OF REQUIRED METHOD RECORDS
954
914(o)
ACCESS TAG TO CONTROL MODIFICATION OF THIS RECORD
956
REQUIRED METHOD RECORD 1
924(o)(a)
LENGTH OF THIS RECORD
958
NUMBER OF METHOD OPTION RECORDS
960
ACCESS TAG TO CONTROL MODIFICATION OF THIS RECORD
962
METHOD OPTION RECORD 1
924(o)(a)(1)
LENGTH OF THIS RECORD
964
LENGTH OF DATA AREA
966
METHOD ID (TYPE/OWNER/CLASS/INSTANCE)
968
CORRELATION TAG FOR CORRELATION WITH REQUIRED METHOD
970
ACCESS TAG TO CONTROL MODIFICATION OF THIS RECORD
972
METHOD SPECIFIC ATTRIBUTES
974
DATA AREA
976
CHECK VALUE
978
924(o)(a)(2)
METHOD OPTION RECORD 2
920(o)(b)
REQUIRED METHOD RECORD 2
CHECK VALUE
906a
RIGHTS RECORD 1
906b
RIGHTS RECORD 2
CHECK VALUE
980

PERC

FIG. 26B



PERC RIGHTS RECORD

FIG. 27
SHIPPING TABLE

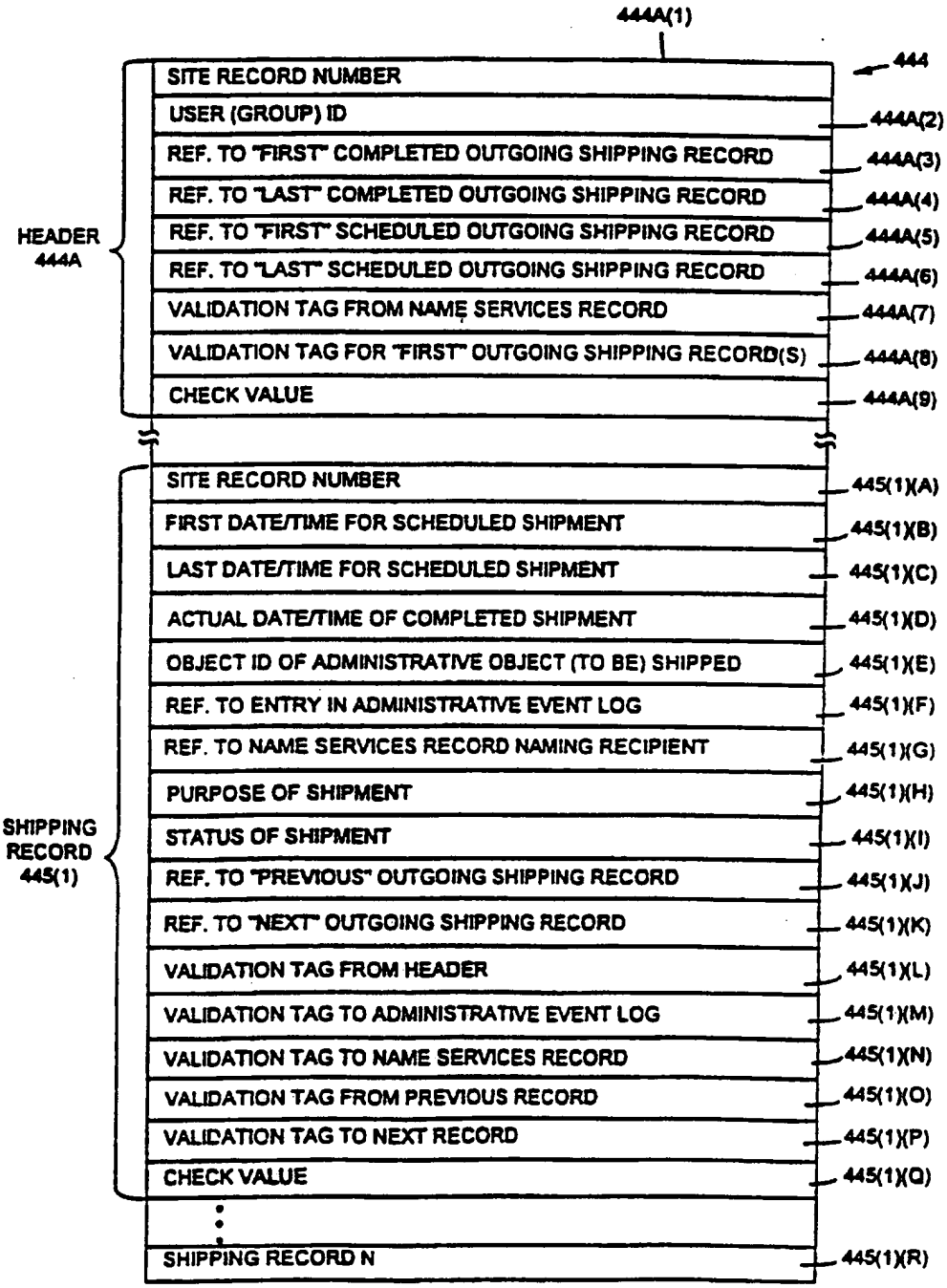


FIG. 28
RECEIVING TABLE

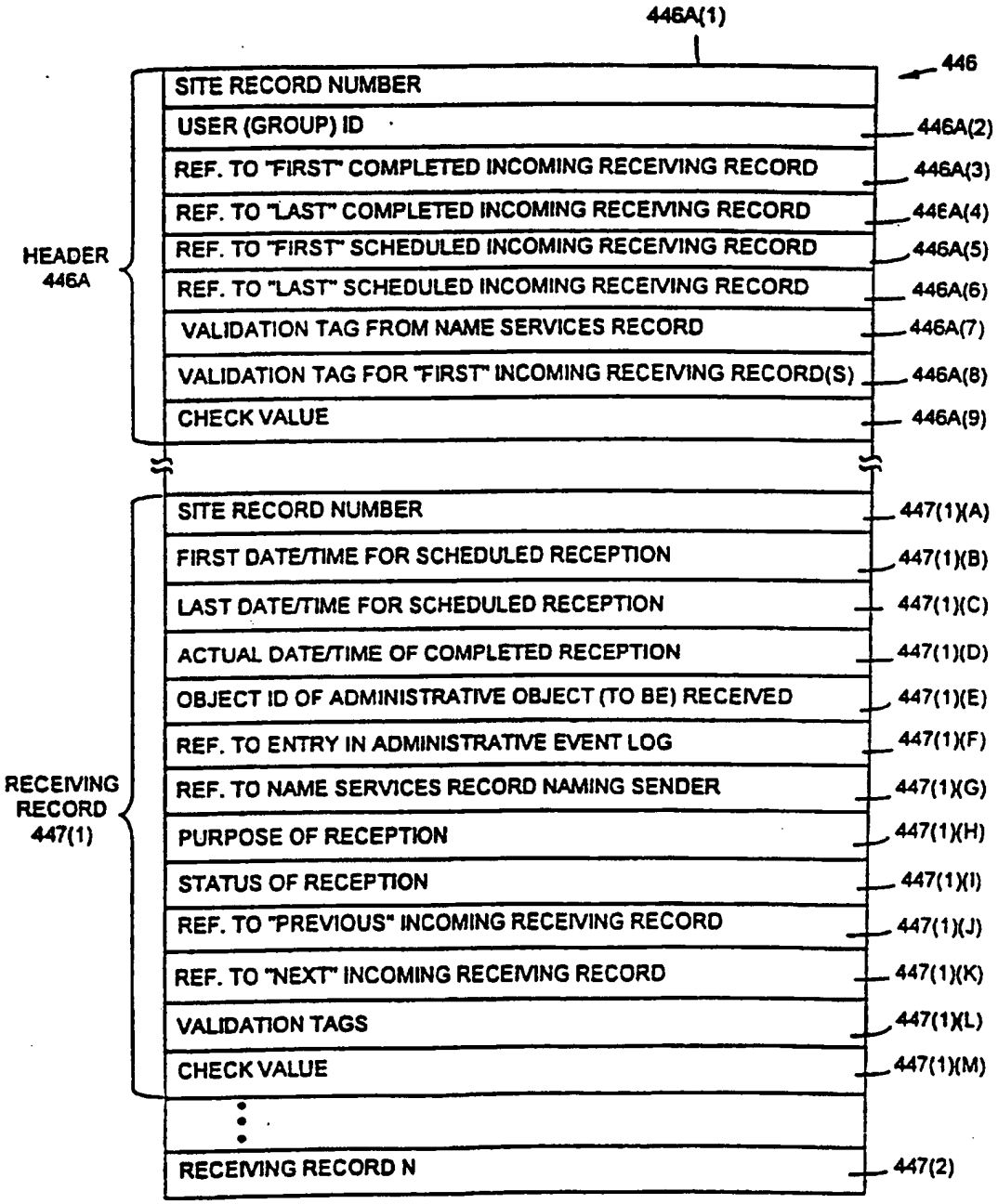
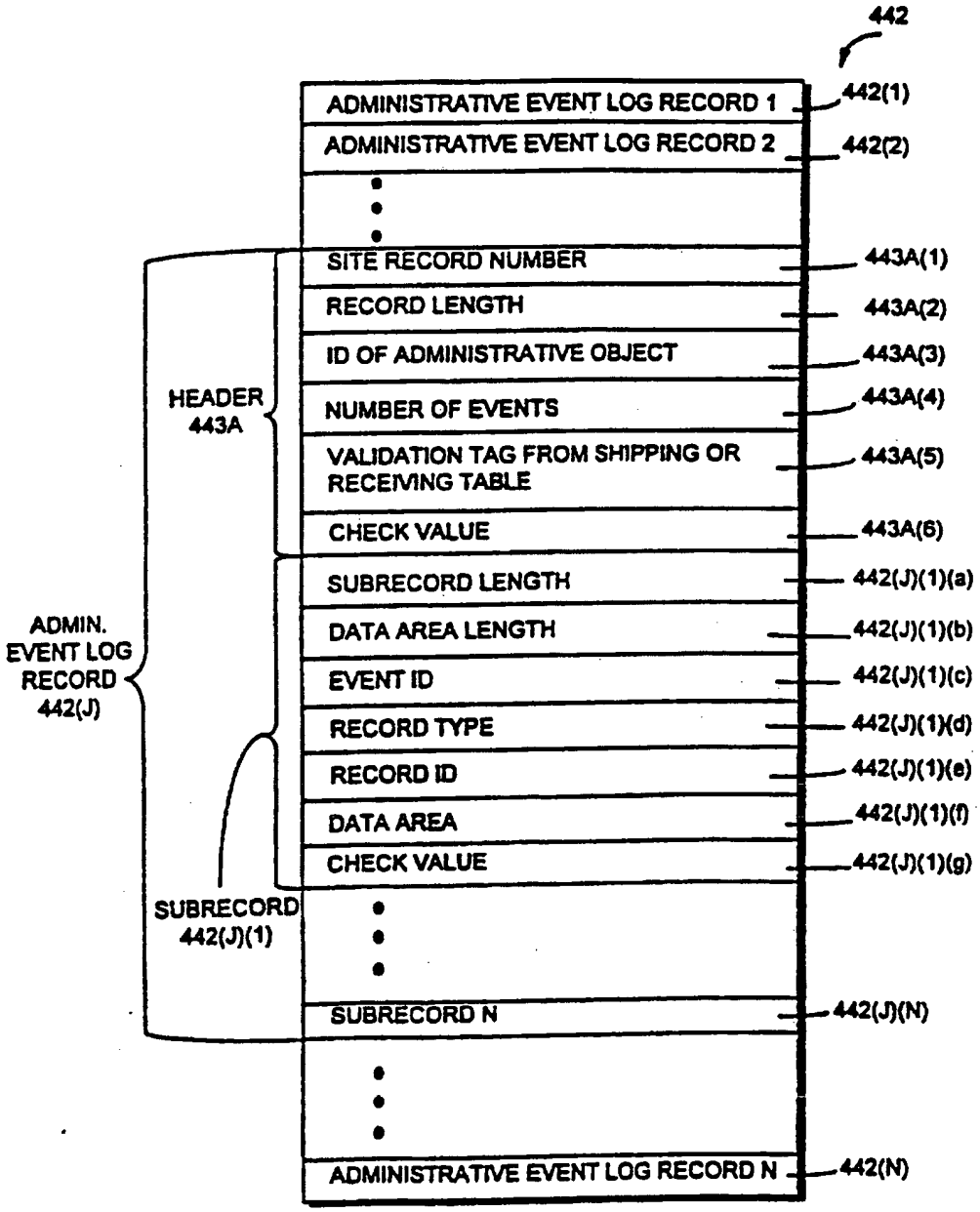


FIG. 29
ADMINISTRATIVE EVENT LOG



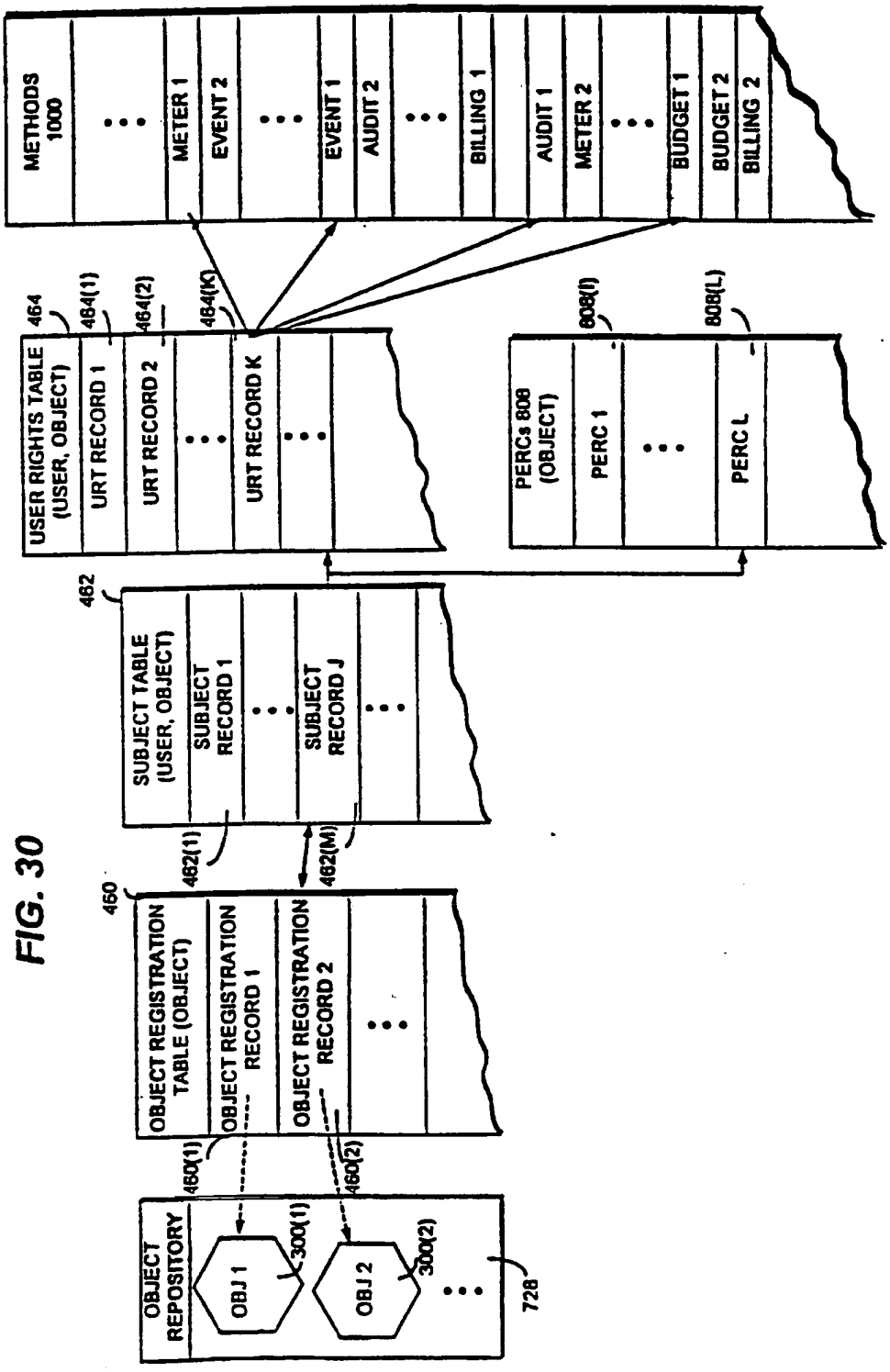

METHODS 1000
METER 1
EVENT 2
EVENT 1
AUDIT 2
BILLING 1
AUDIT 1
METER 2
BUDGET 1
BUDGET 2
BILLING 2
USER RIGHTS TABLE (USER, OBJECT)
464
464(1)
464(2)
464(K)
URT RECORD 1
URT RECORD 2
URT RECORD K
PERCs 808 (OBJECT)
808(1)
808(L)
PERC 1
PERC L
SUBJECT TABLE (USER, OBJECT)
462
SUBJECT RECORD 1
SUBJECT RECORD J
462(1)
462(M)
OBJECT REGISTRATION TABLE (OBJECT)
460
OBJECT REGISTRATION RECORD 1
OBJECT REGISTRATION RECORD 2
460(1)
460(2)
OBJECT REPOSITORY
OBJ 1
OBJ 2
300(1)
300(2)
728

FIG. 30

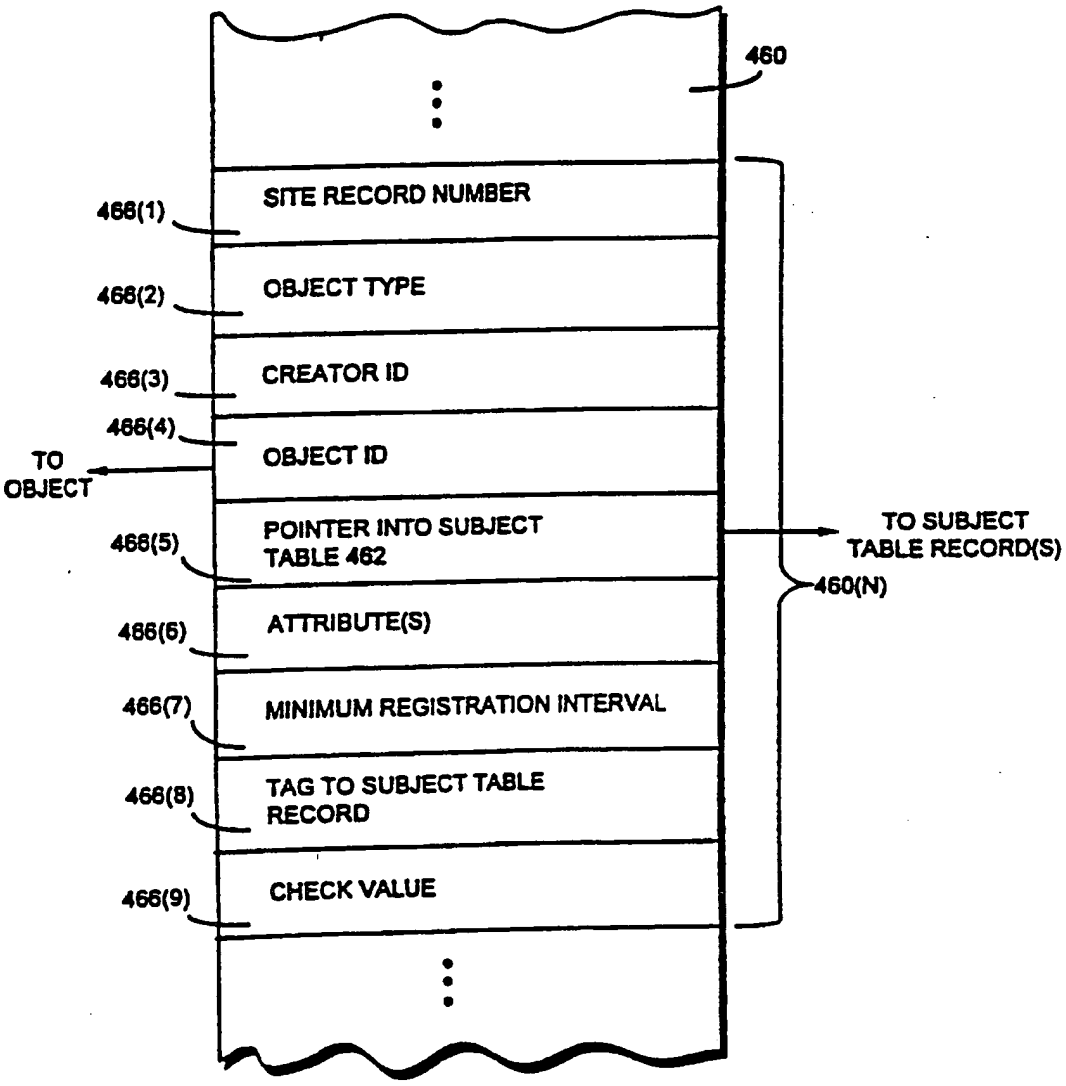


FIG. 31
OBJECT REGISTRATION TABLE

FIG. 32

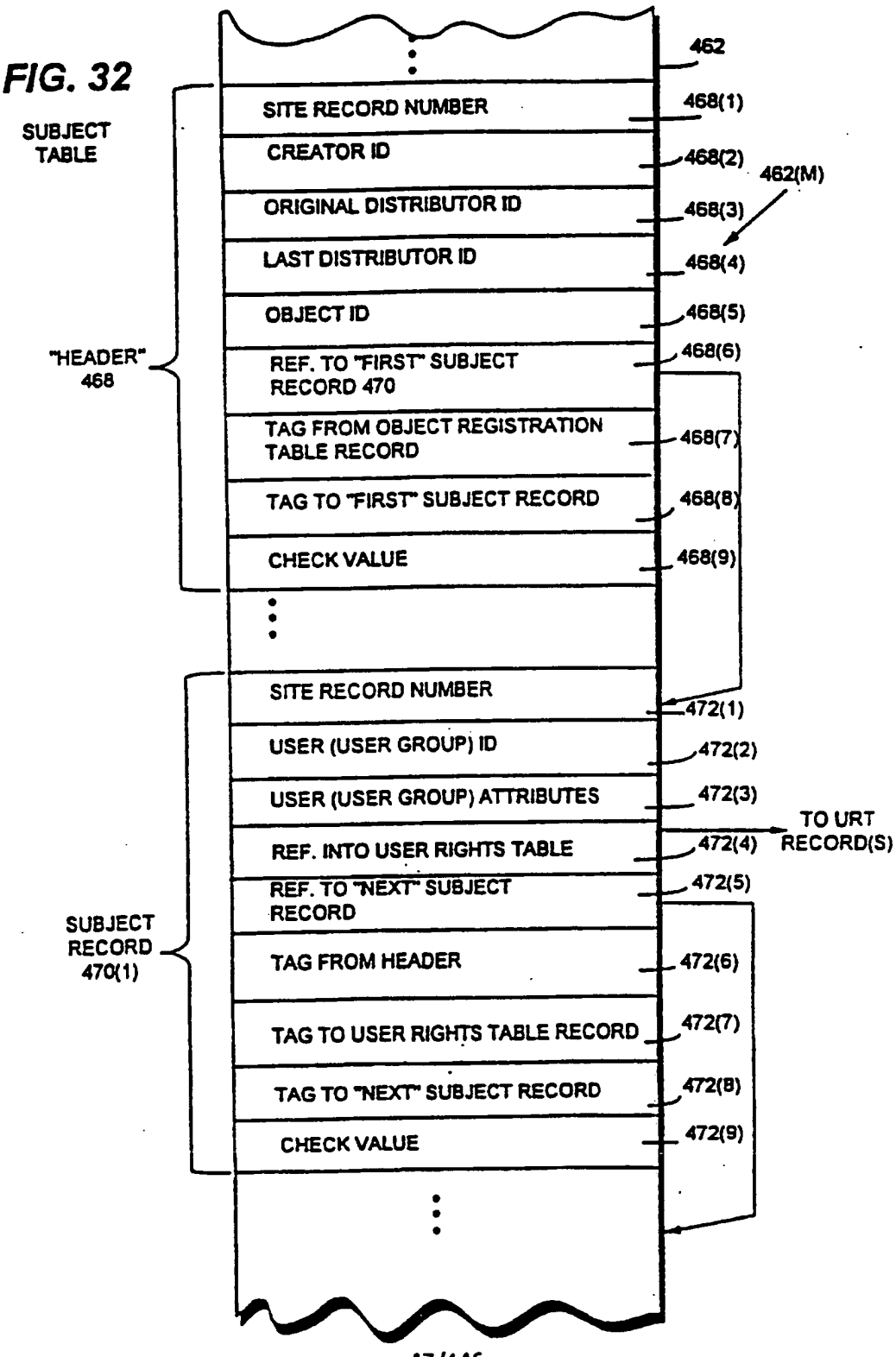

SUBJECT TABLE
462
SITE RECORD NUMBER
468(1)
CREATOR ID
468(2)
462(M)
ORIGINAL DISTRIBUTOR ID
468(3)
LAST DISTRIBUTOR ID
468(4)
OBJECT ID
468(5)
"HEADER" 468
REF. TO "FIRST" SUBJECT RECORD 470
468(6)
TAG FROM OBJECT REGISTRATION TABLE RECORD
468(7)
TAG TO "FIRST" SUBJECT RECORD
468(8)
CHECK VALUE
468(9)
SITE RECORD NUMBER
472(1)
USER (USER GROUP) ID
472(2)
USER (USER GROUP) ATTRIBUTES
472(3)
REF. INTO USER RIGHTS TABLE
472(4)
TO URT RECORD(S)
REF. TO "NEXT" SUBJECT RECORD
472(5)
SUBJECT RECORD 470(1)
TAG FROM HEADER
472(6)
TAG TO USER RIGHTS TABLE RECORD
472(7)
TAG TO "NEXT" SUBJECT RECORD
472(8)
CHECK VALUE
472(9)

FIG. 33 USER RIGHTS TABLE

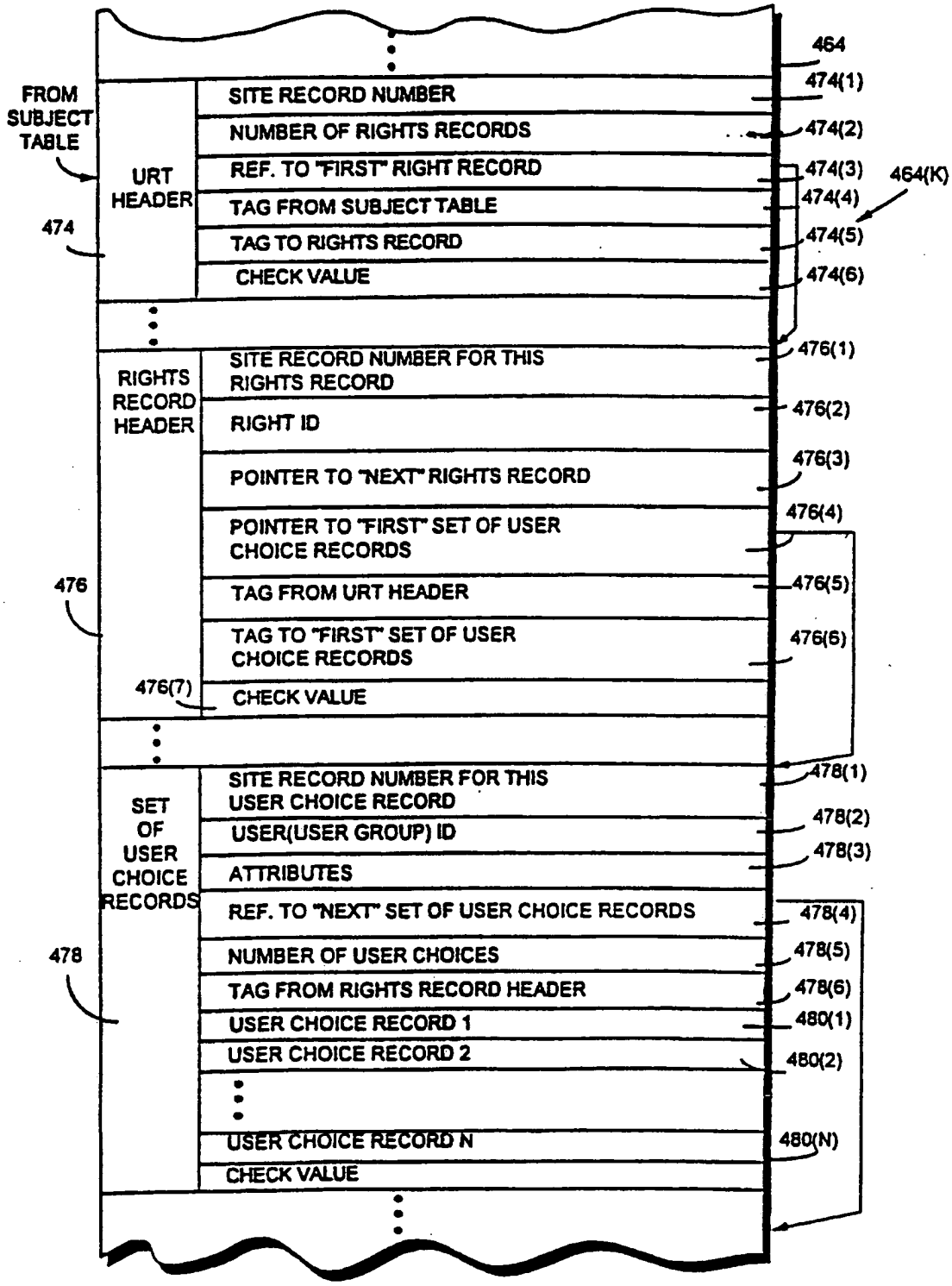


FIG. 34

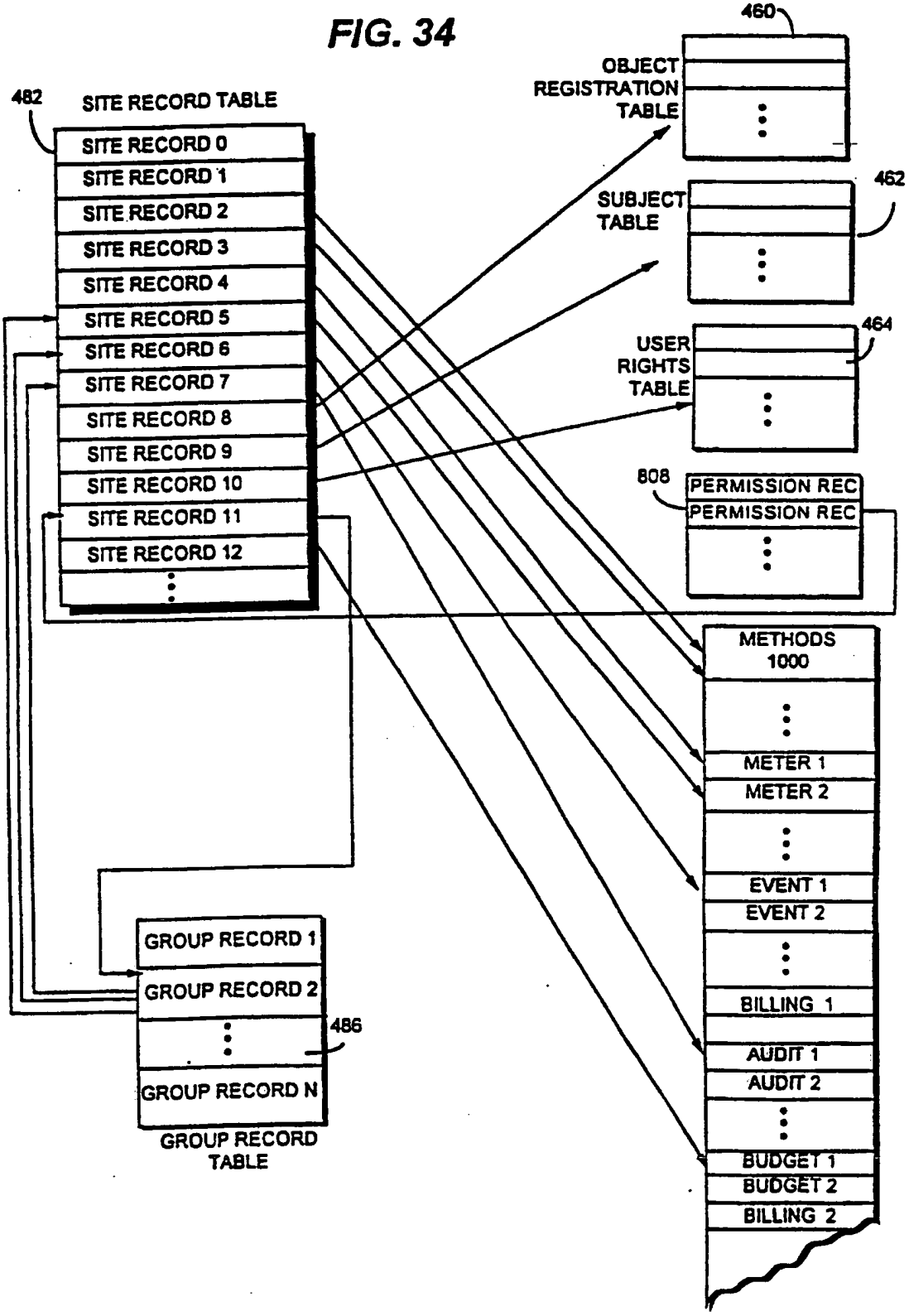

460
OBJECT REGISTRATION TABLE
462
SUBJECT TABLE
464
USER RIGHTS TABLE
808
PERMISSION REC
PERMISSION REC
482
SITE RECORD TABLE
SITE RECORD 0
SITE RECORD 1
SITE RECORD 2
SITE RECORD 3
SITE RECORD 4
SITE RECORD 5
SITE RECORD 6
SITE RECORD 7
SITE RECORD 8
SITE RECORD 9
SITE RECORD 10
SITE RECORD 11
SITE RECORD 12
METHODS 1000
METER 1
METER 2
EVENT 1
EVENT 2
BILLING 1
AUDIT 1
AUDIT 2
BUDGET 1
BUDGET 2
BILLING 2
GROUP RECORD 1
GROUP RECORD 2
GROUP RECORD N
486
GROUP RECORD TABLE

FIG. 34A

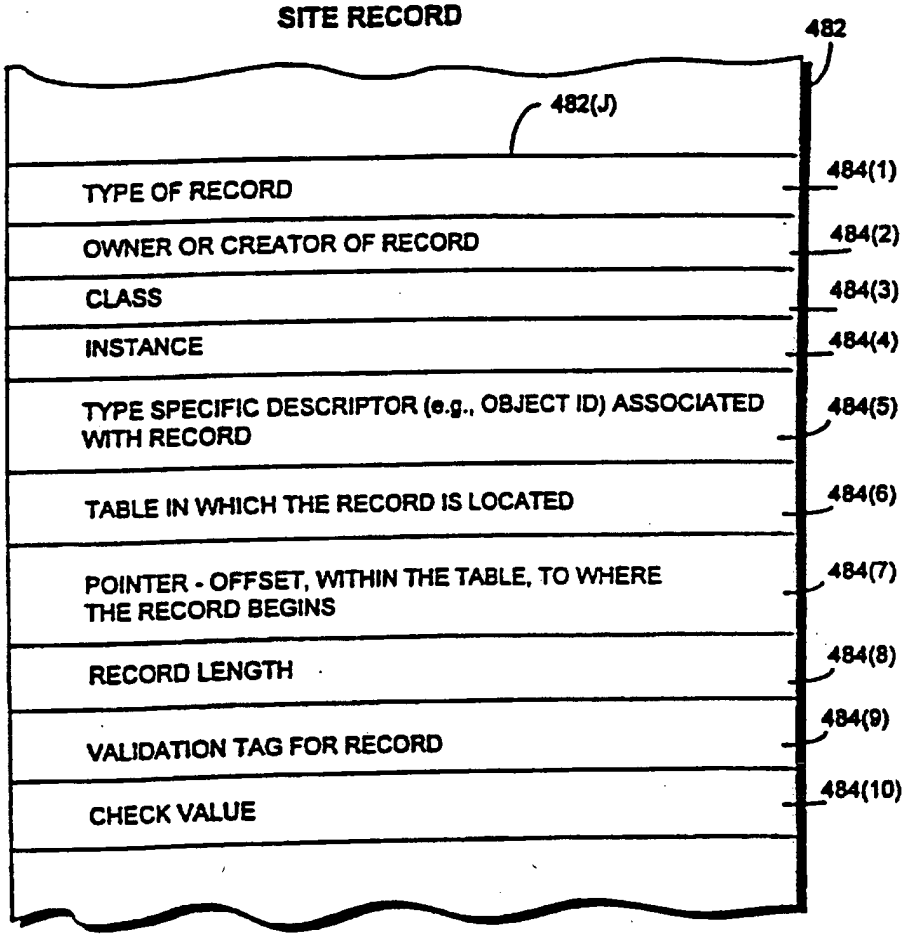

SITE RECORD
482
482(J)
TYPE OF RECORD
484(1)
OWNER OR CREATOR OF RECORD
484(2)
CLASS
484(3)
INSTANCE
484(4)
TYPE SPECIFIC DESCRIPTOR (e.g., OBJECT ID) ASSOCIATED WITH RECORD
484(5)
TABLE IN WHICH THE RECORD IS LOCATED
484(6)
POINTER - OFFSET, WITHIN THE TABLE, TO WHERE THE RECORD BEGINS
484(7)
RECORD LENGTH
484(8)
VALIDATION TAG FOR RECORD
484(9)
CHECK VALUE
484(10)

FIG. 34B

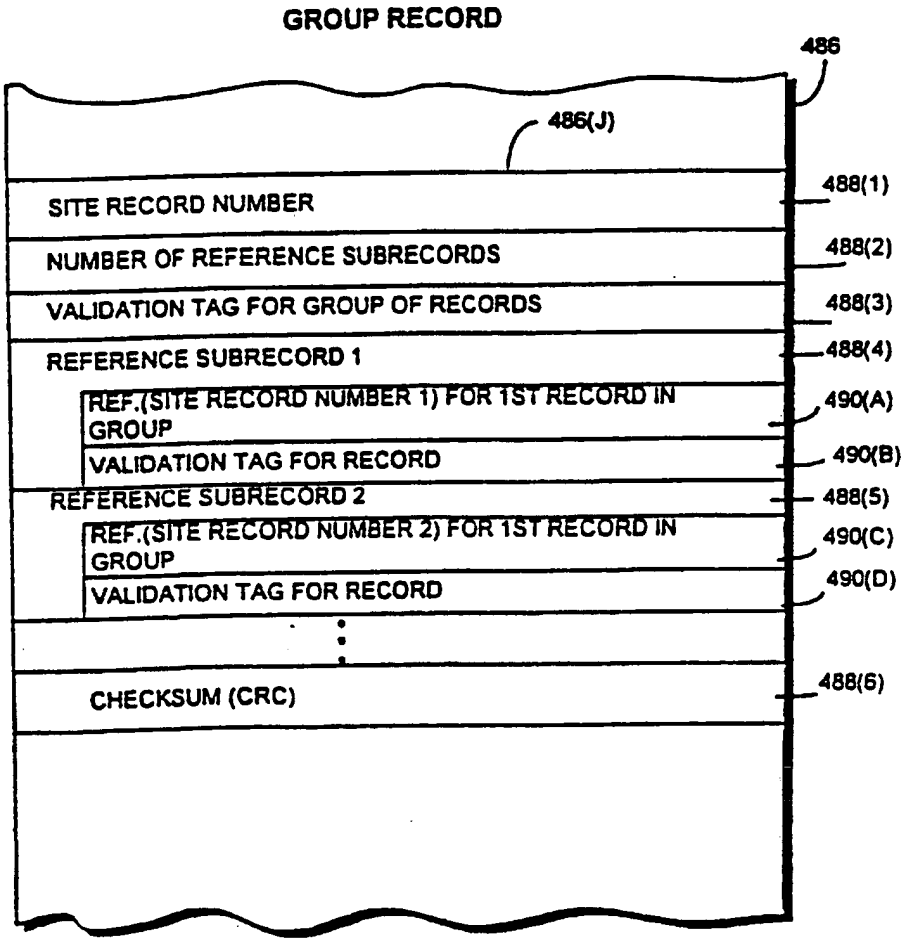

GROUP RECORD
486
486(J)
SITE RECORD NUMBER
488(1)
NUMBER OF REFERENCE SUBRECORDS
488(2)
VALIDATION TAG FOR GROUP OF RECORDS
488(3)
REFERENCE SUBRECORD 1
488(4)
REF.(SITE RECORD NUMBER 1) FOR 1ST RECORD IN GROUP
490(A)
VALIDATION TAG FOR RECORD
490(B)
REFERENCE SUBRECORD 2
488(5)
REF.(SITE RECORD NUMBER 2) FOR 1ST RECORD IN GROUP
490(C)
VALIDATION TAG FOR RECORD
490(D)
CHECKSUM (CRC)
488(6)

FIG. 35

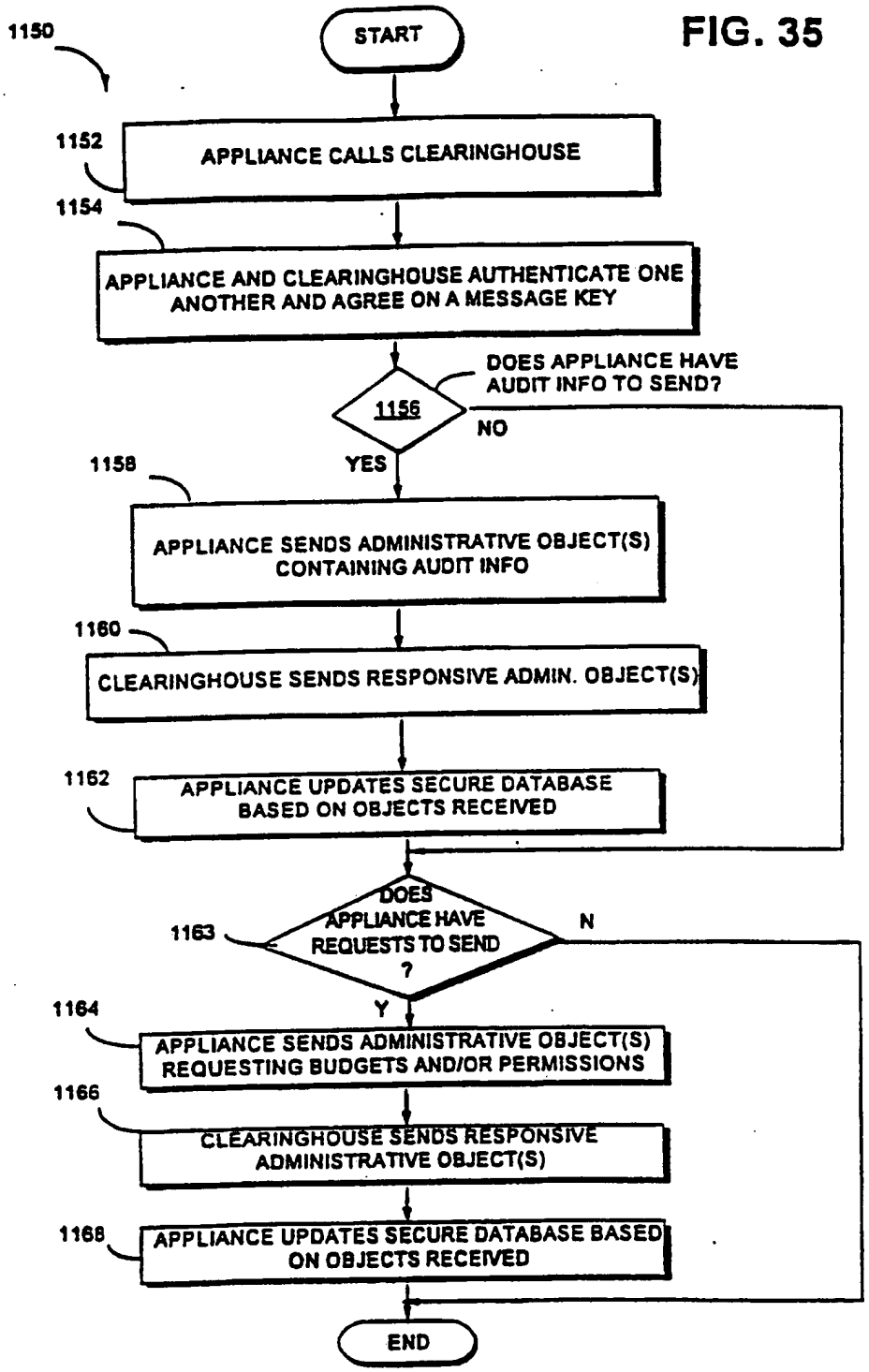

1150
START
1152
APPLIANCE CALLS CLEARINGHOUSE
1154
APPLIANCE AND CLEARINGHOUSE AUTHENTICATE ONE ANOTHER AND AGREE ON A MESSAGE KEY
DOES APPLIANCE HAVE AUDIT INFO TO SEND?
1156
NO
YES
1158
APPLIANCE SENDS ADMINISTRATIVE OBJECT(S) CONTAINING AUDIT INFO
1160
CLEARINGHOUSE SENDS RESPONSIVE ADMIN. OBJECT(S)
1162
APPLIANCE UPDATES SECURE DATABASE BASED ON OBJECTS RECEIVED
1163
DOES APPLIANCE HAVE REQUESTS TO SEND ?
N
Y
1164
APPLIANCE SENDS ADMINISTRATIVE OBJECT(S) REQUESTING BUDGETS AND/OR PERMISSIONS
1166
CLEARINGHOUSE SENDS RESPONSIVE ADMINISTRATIVE OBJECT(S)
1168
APPLIANCE UPDATES SECURE DATABASE BASED ON OBJECTS RECEIVED
END

FIG. 36

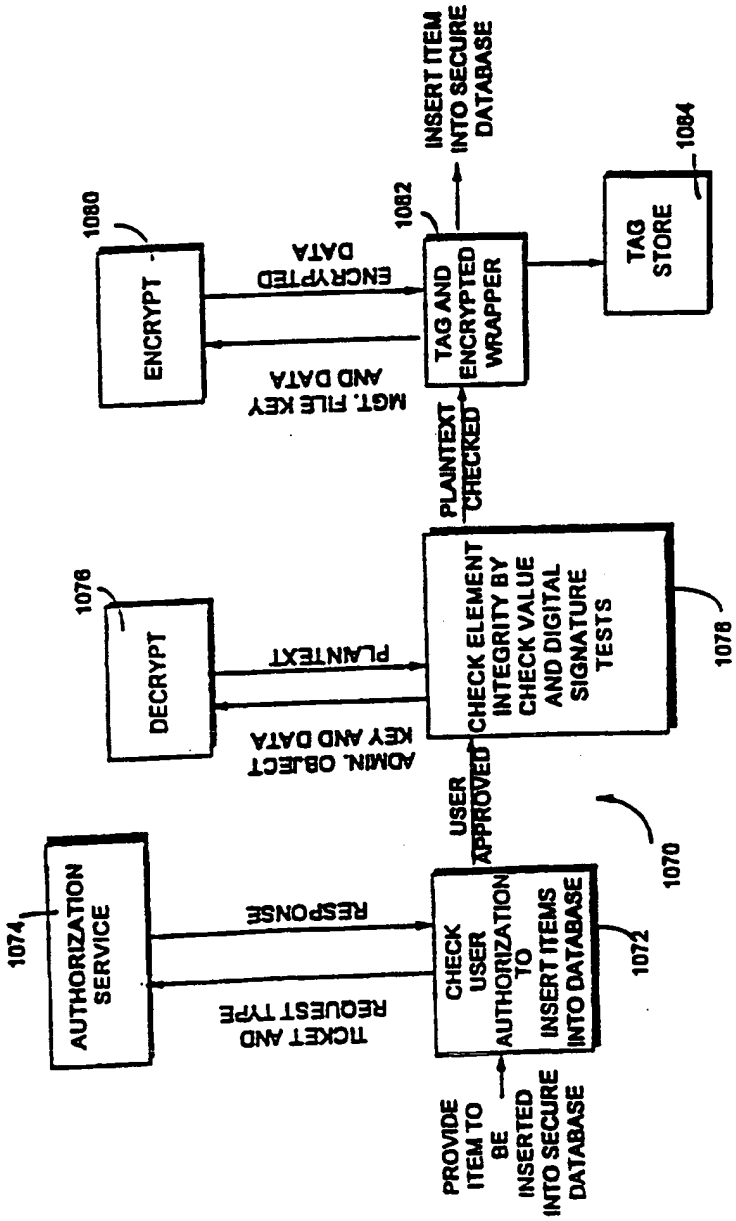

PROVIDE ITEM TO BE INSERTED INTO SECURE DATABASE
CHECK USER AUTHORIZATION TO INSERT ITEMS INTO DATABASE
1072
1070
AUTHORIZATION SERVICE
1074
REQUEST TYPE AND TICKET
RESPONSE
USER APPROVED
DECRYPT
1076
ADMIN. OBJECT KEY AND DATA
PLAINTEXT
CHECK ELEMENT INTEGRITY BY CHECK VALUE AND DIGITAL SIGNATURE TESTS
1078
PLAINTEXT CHECKED
ENCRYPT
1080
MGT. FILE KEY AND DATA
ENCRYPTED DATA
TAG AND ENCRYPTED WRAPPER
1082
INSERT ITEM INTO SECURE DATABASE
TAG STORE
1084

FIG. 37

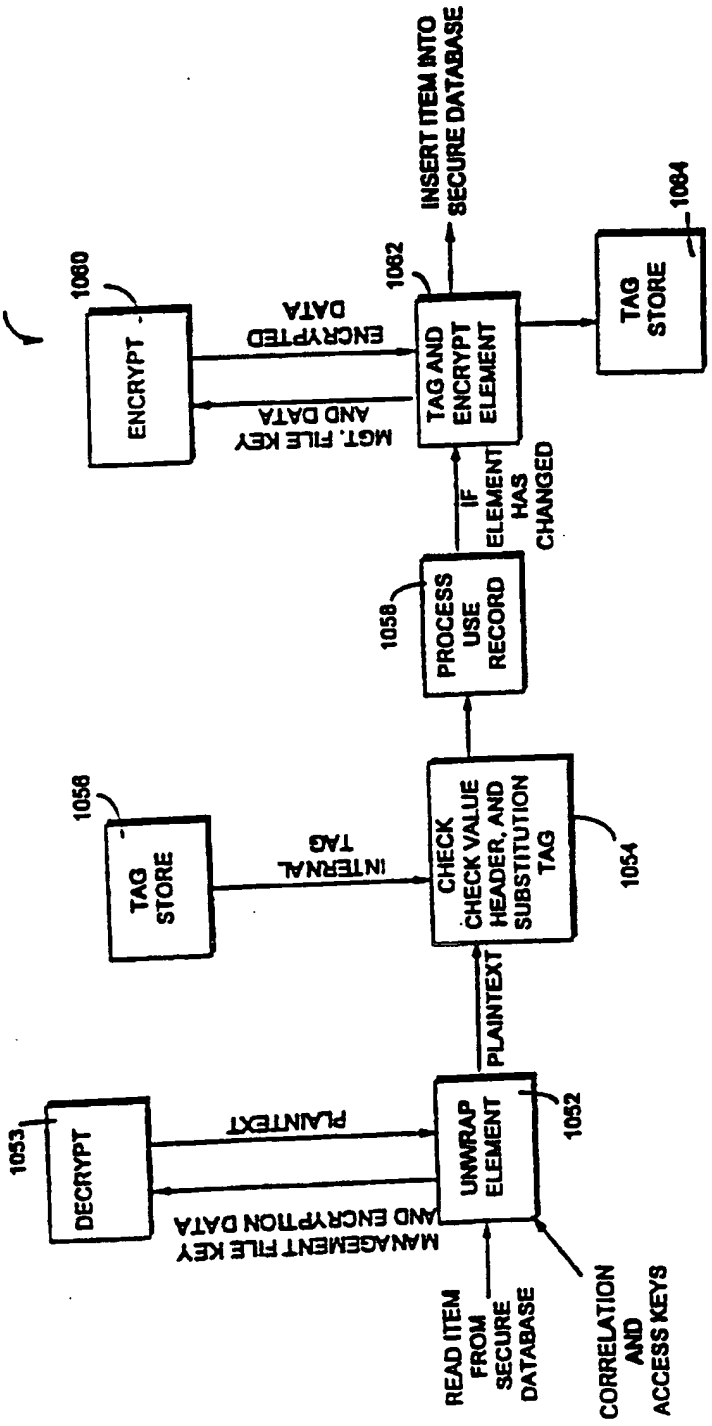

1050
1060
ENCRYPT
ENCRYPTED DATA
MGT. FILE KEY AND DATA
1062
TAG AND ENCRYPT ELEMENT
INSERT ITEM INTO SECURE DATABASE
1064
TAG STORE
IF ELEMENT HAS CHANGED
1056
PROCESS USE RECORD
1058
TAG STORE
INTERNAL TAG
CHECK CHECK VALUE HEADER, AND SUBSTITUTION TAG
1054
PLAINTEXT
1053
DECRYPT
PLAINTEXT
MANAGEMENT FILE KEY AND ENCRYPTION DATA
UNWRAP ELEMENT
1052
READ ITEM FROM SECURE DATABASE
CORRELATION AND ACCESS KEYS

FIG. 38

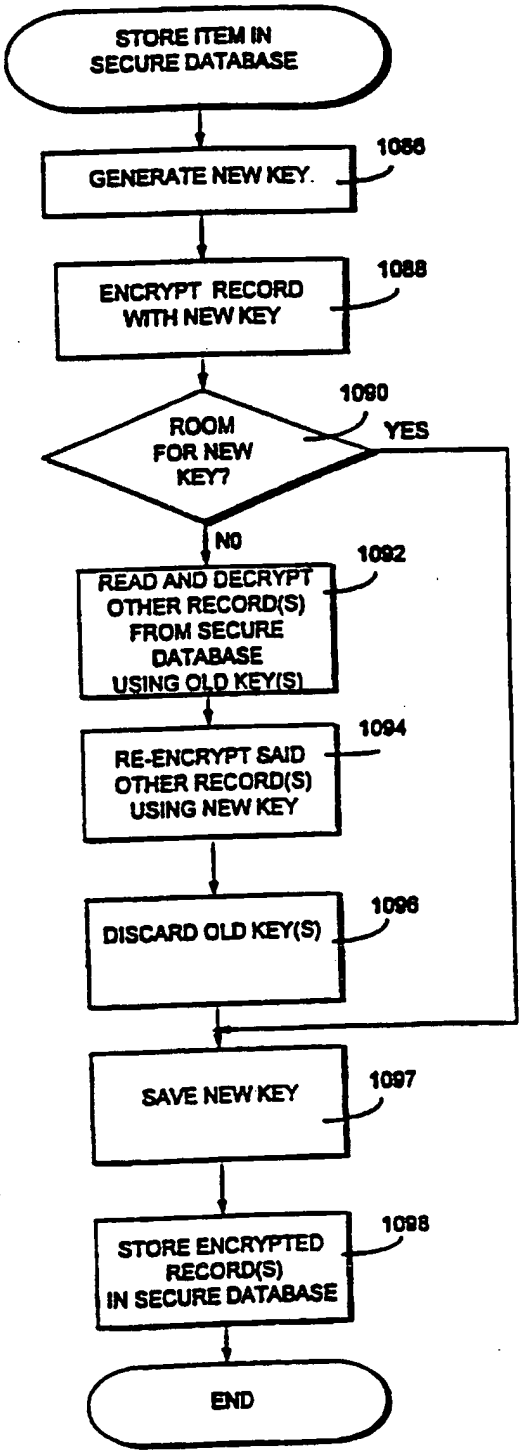

STORE ITEM IN SECURE DATABASE
GENERATE NEW KEY.
1086
ENCRYPT RECORD WITH NEW KEY
1088
ROOM FOR NEW KEY?
1090
YES
NO
READ AND DECRYPT OTHER RECORD(S) FROM SECURE DATABASE USING OLD KEY(S)
1092
RE-ENCRYPT SAID OTHER RECORD(S) USING NEW KEY
1094
DISCARD OLD KEY(S)
1096
SAVE NEW KEY
1097
STORE ENCRYPTED RECORD(S) IN SECURE DATABASE
1098
END

FIG. 39
BACKUP

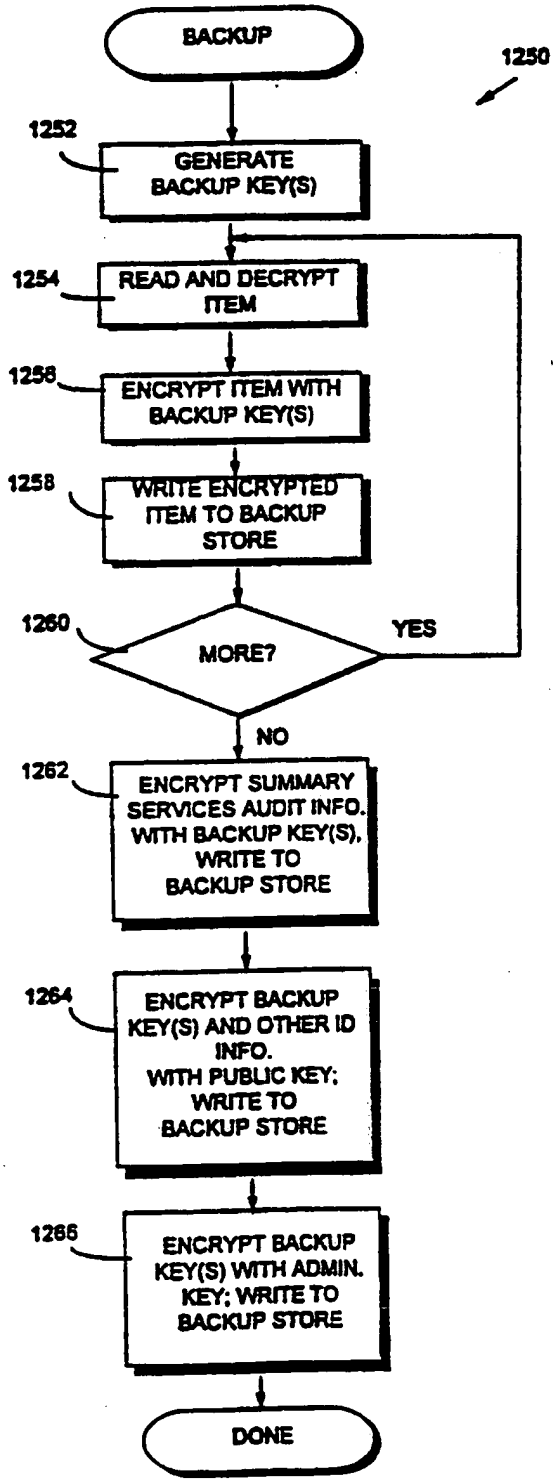
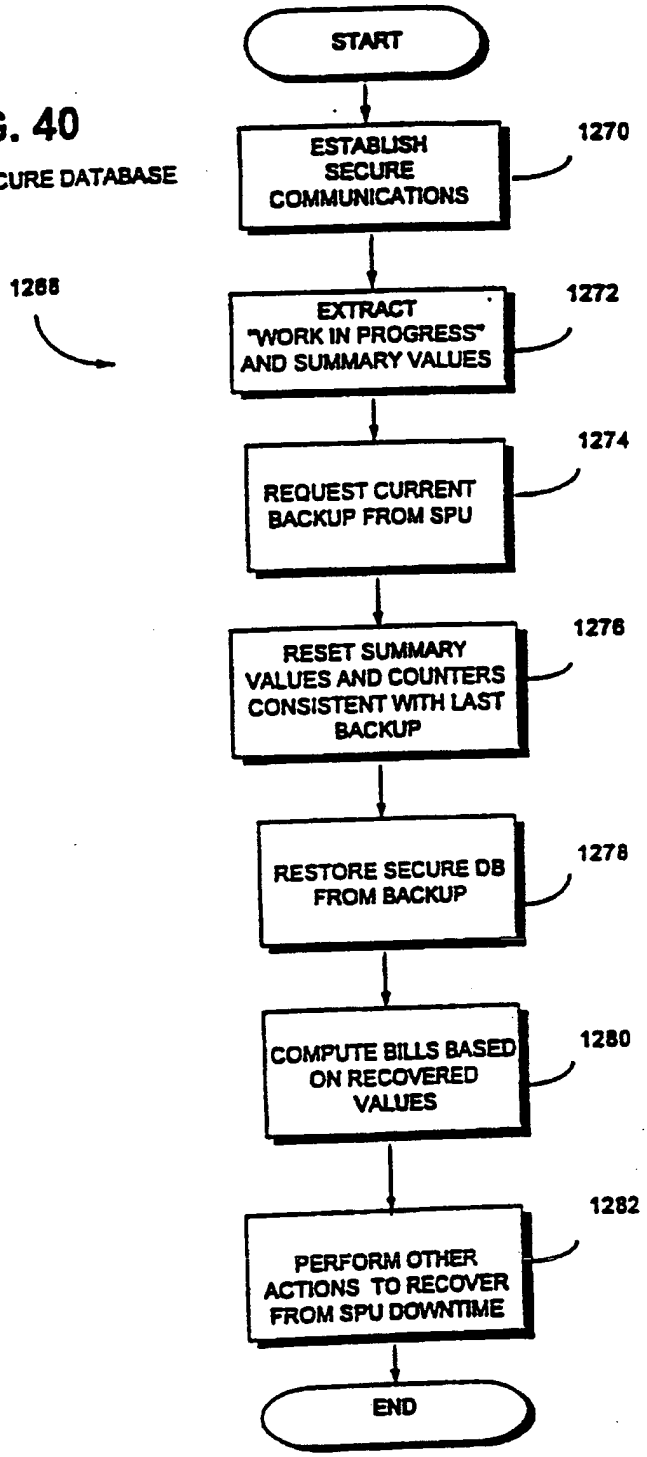


FIG. 40

RECOVER SECURE DATABASE



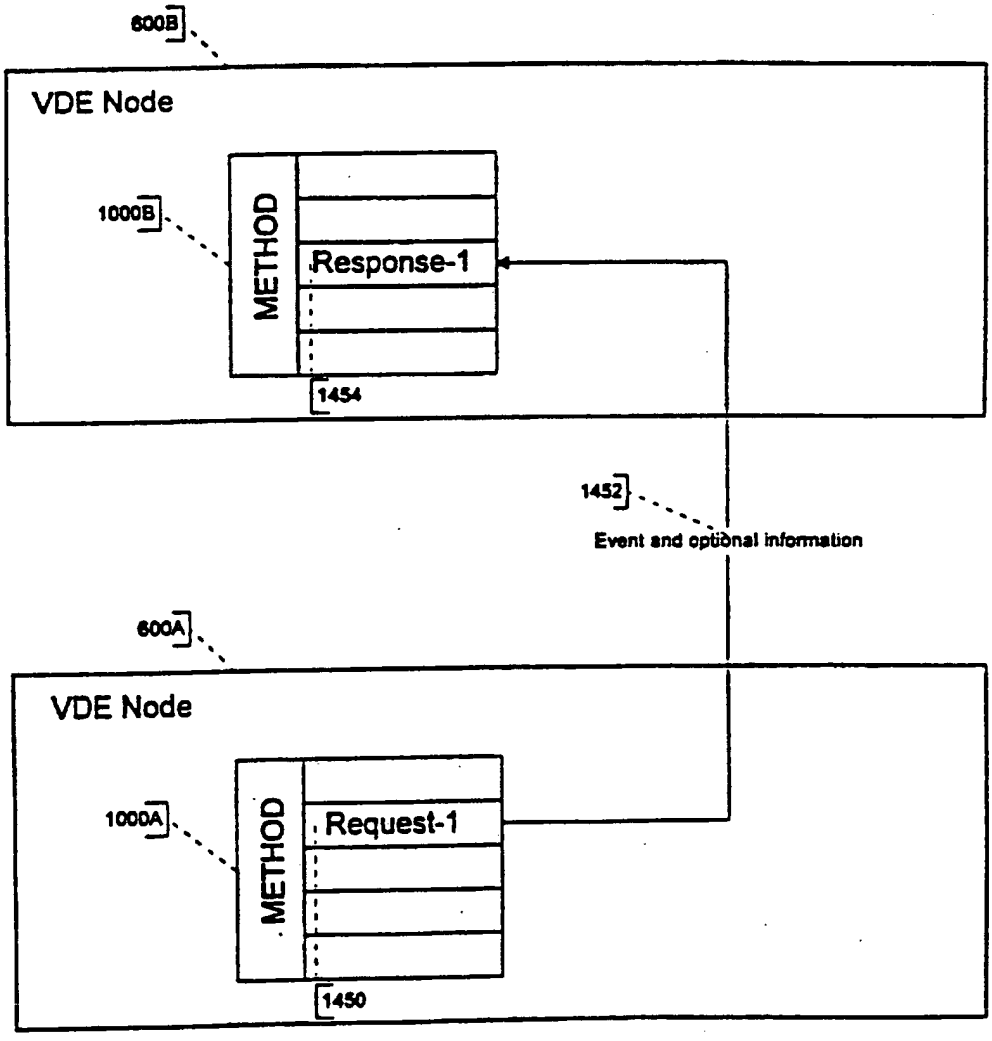

600B
VDE Node
1000B
METHOD
Response-1
1454
1452
Event and optional information
600A
VDE Node
1000A
METHOD
Request-1
1450

Figure 41a

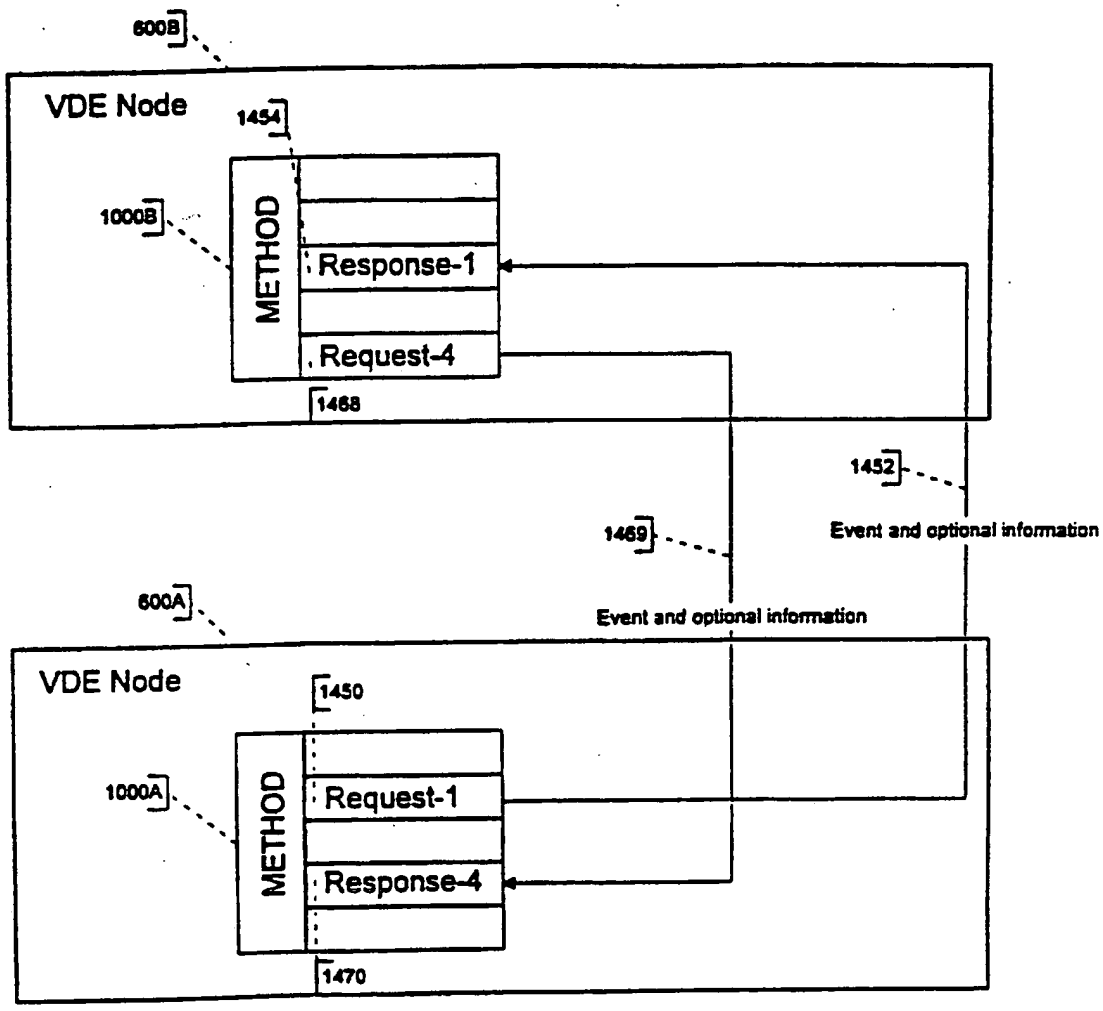

600B
VDE Node
1454
1000B
METHOD
Response-1
Request-4
1468
1452
Event and optional information
1469
Event and optional information
600A
VDE Node
1450
1000A
METHOD
Request-1
Response-4
1470

Figure 41b

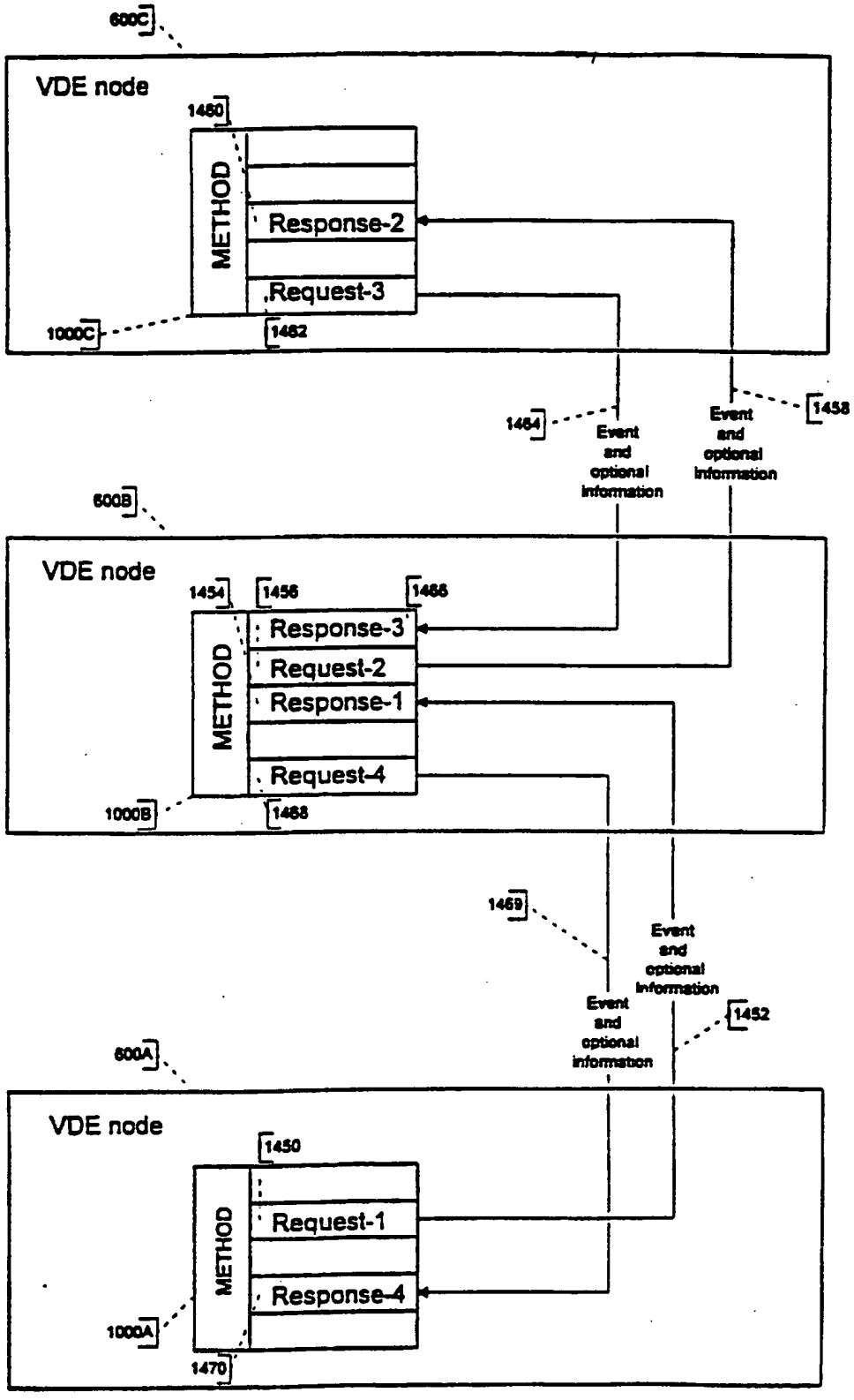

600C
VDE node
1480
METHOD
Response-2
Request-3
1000C
1482
1464
Event and optional information
1458
Event and optional information
600B
VDE node
1454
1456
1466
Response-3
Request-2
Response-1
Request-4
1000B
1468
1469
Event and optional information
Event and optional information
1452
600A
VDE node
1450
Request-1
Response-4
1000A
1470

Figure 41c

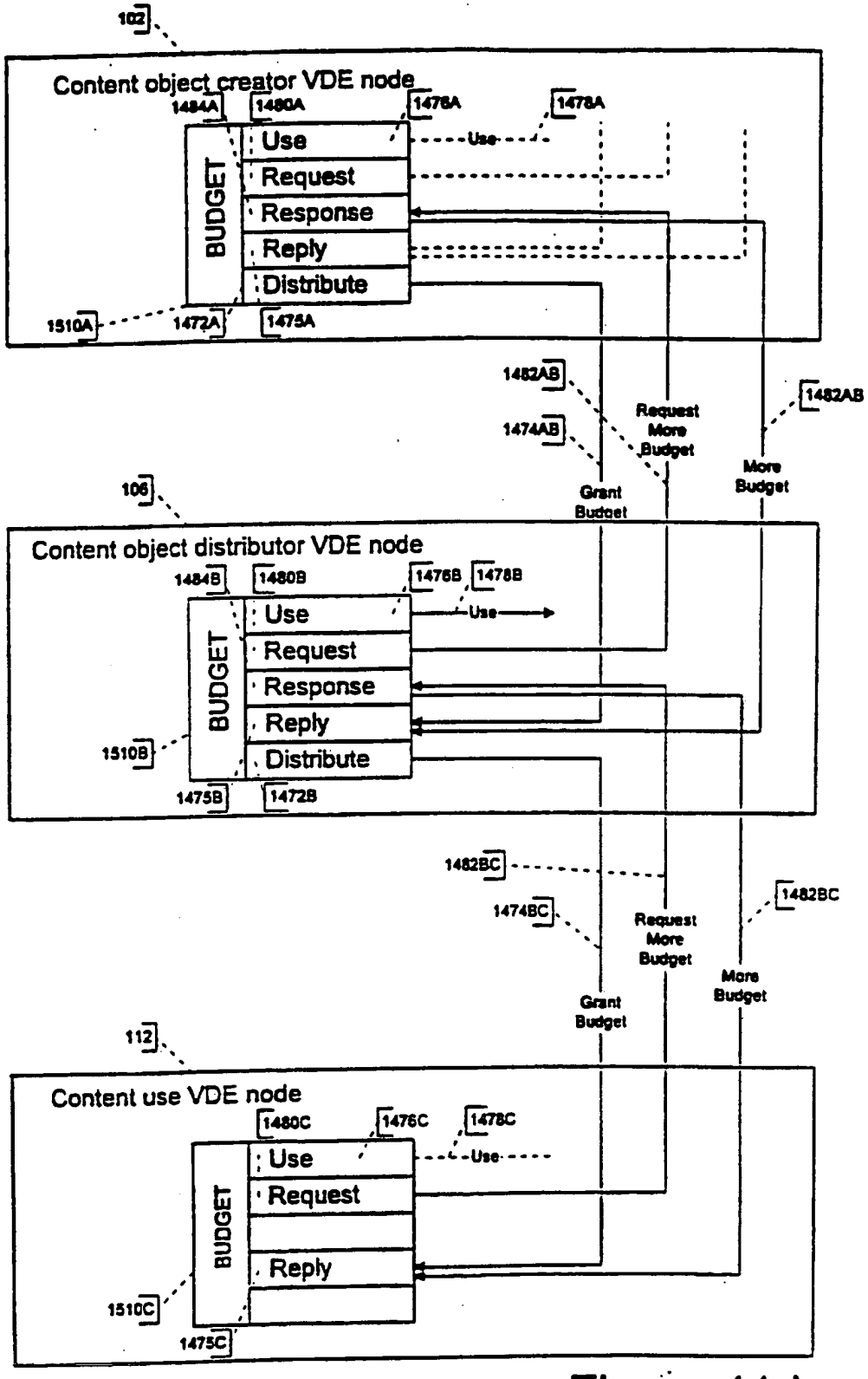

102
Content object creator VDE node
1484A
1480A
1476A
1478A
Use
Request
Response
Reply
Distribute
BUDGET
1510A
1472A
1475A
Use
1482AB
1474AB
Request More Budget
Grant Budget
More Budget
1482AB
106
Content object distributor VDE node
1484B
1480B
1476B
1478B
Use
Request
Response
Reply
Distribute
BUDGET
1510B
1475B
1472B
Use
1482BC
1474BC
Request More Budget
Grant Budget
More Budget
1482BC
112
Content use VDE node
1480C
1476C
1478C
Use
Request
Reply
BUDGET
1510C
1475C
Use

Figure 41d

BUDGET Method Use Process Flow

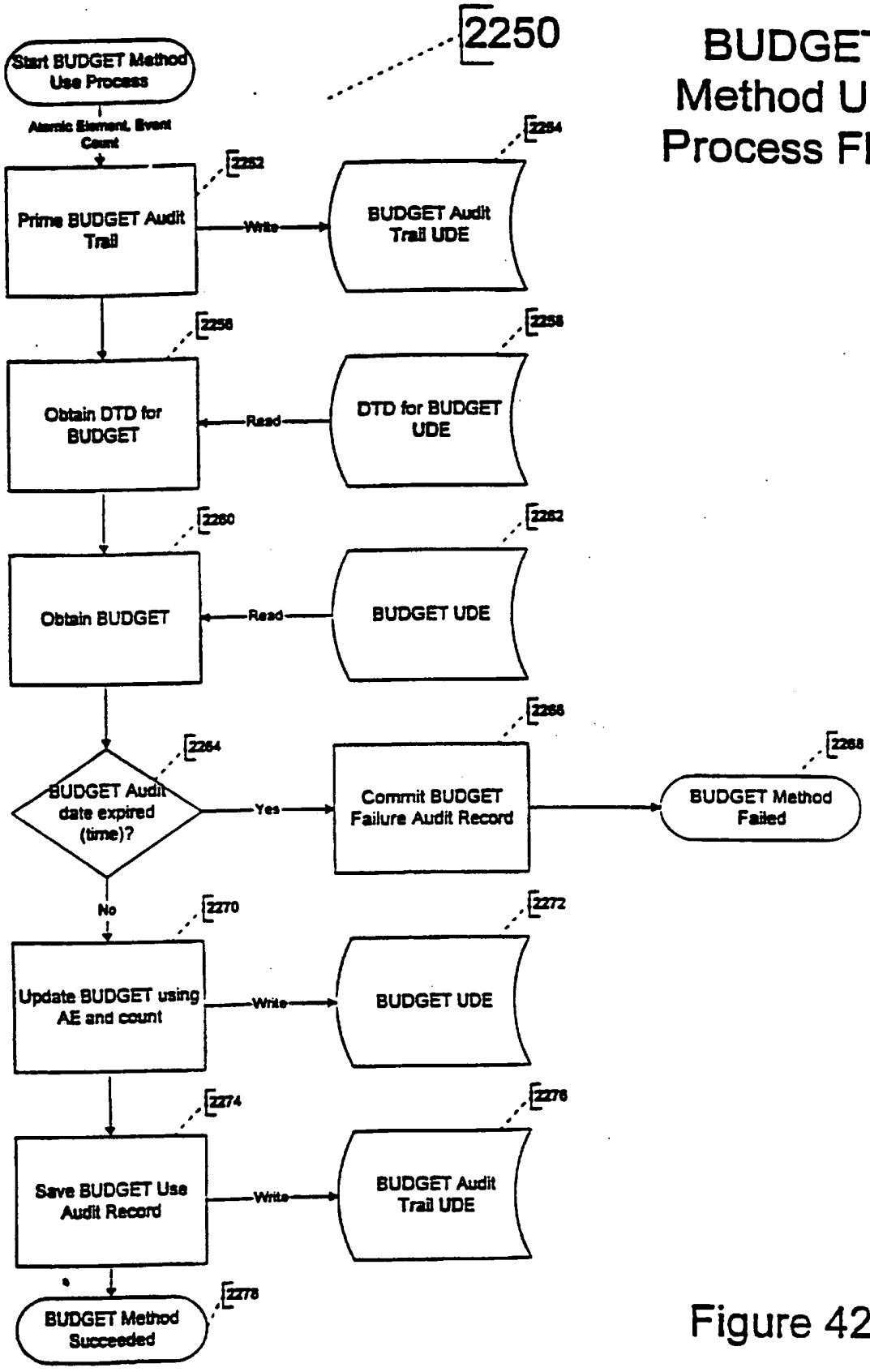


Figure 42a

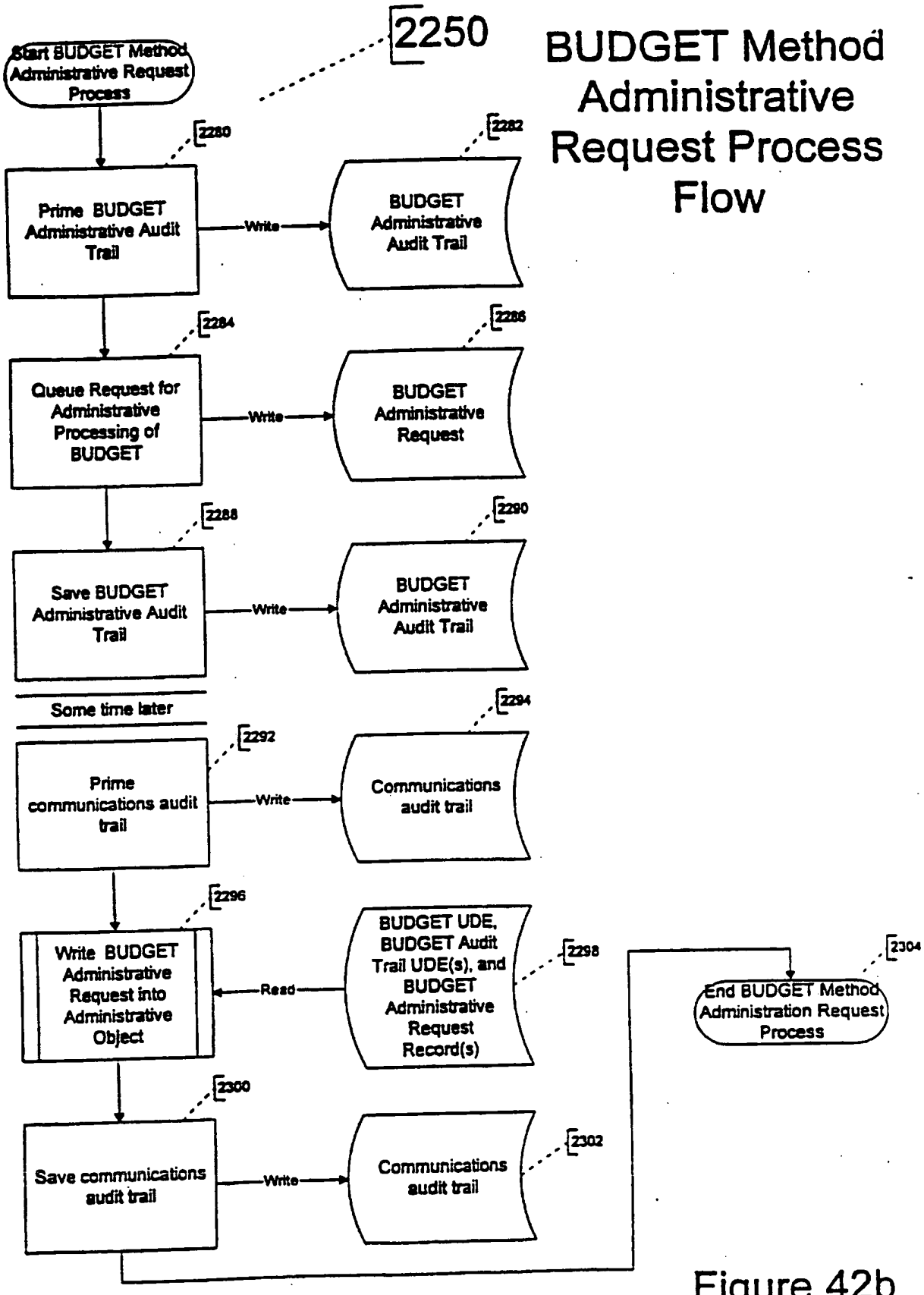

2250
BUDGET Method Administrative Request Process Flow
Start BUDGET Method Administrative Request Process
2280
Prime BUDGET Administrative Audit Trail
Write
2282
BUDGET Administrative Audit Trail
2284
Queue Request for Administrative Processing of BUDGET
Write
2286
BUDGET Administrative Request
2288
Save BUDGET Administrative Audit Trail
Write
2290
BUDGET Administrative Audit Trail
Some time later
2292
Prime communications audit trail
Write
2294
Communications audit trail
2296
Write BUDGET Administrative Request into Administrative Object
Read
BUDGET UDE, BUDGET Audit Trail UDE(s), and BUDGET Administrative Request Record(s)
2298
2300
Save communications audit trail
Write
Communications audit trail
2302
2304
End BUDGET Method Administration Request Process

Figure 42b

BUDGET Method Administrative Response Process Flow

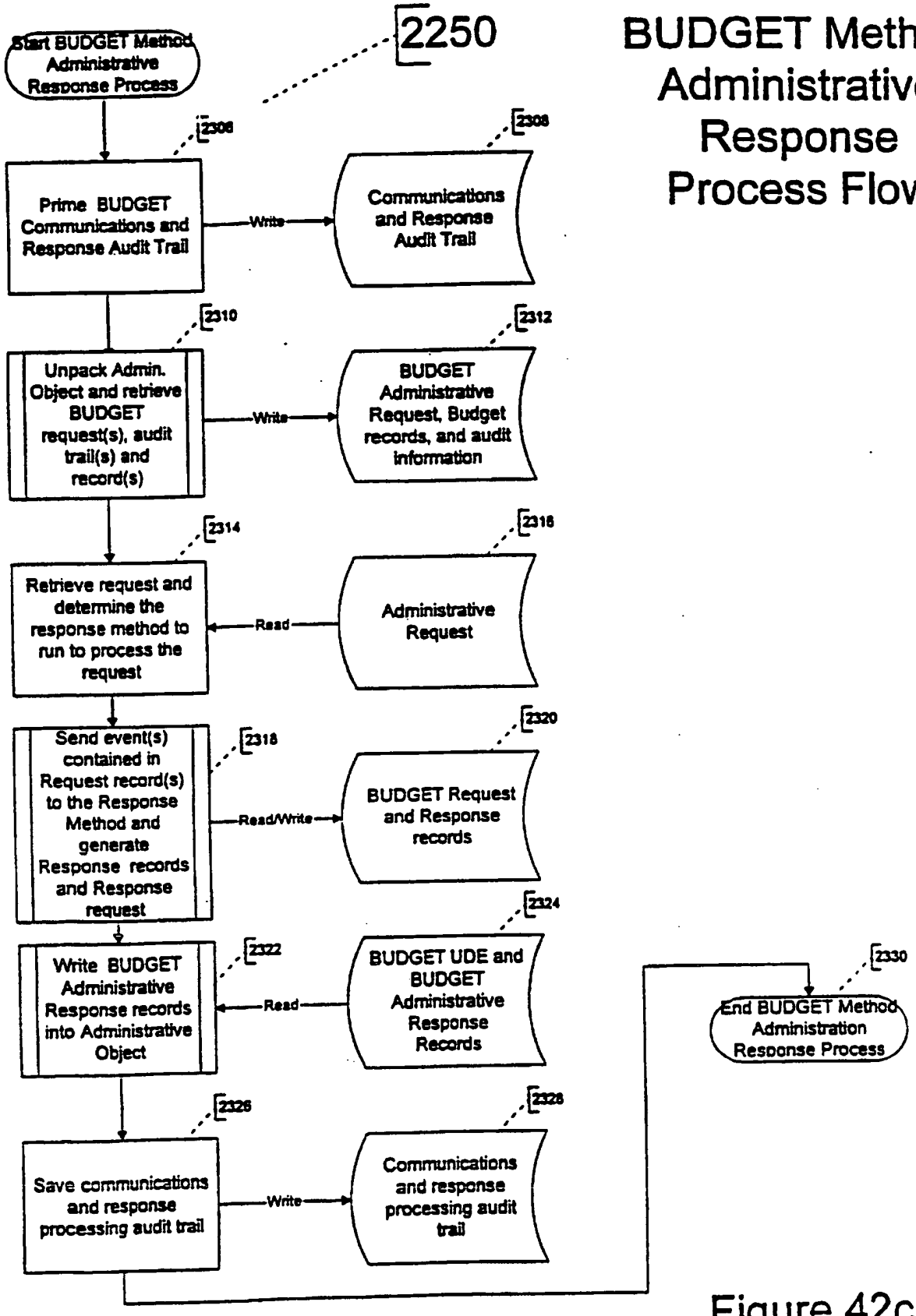


Figure 42c

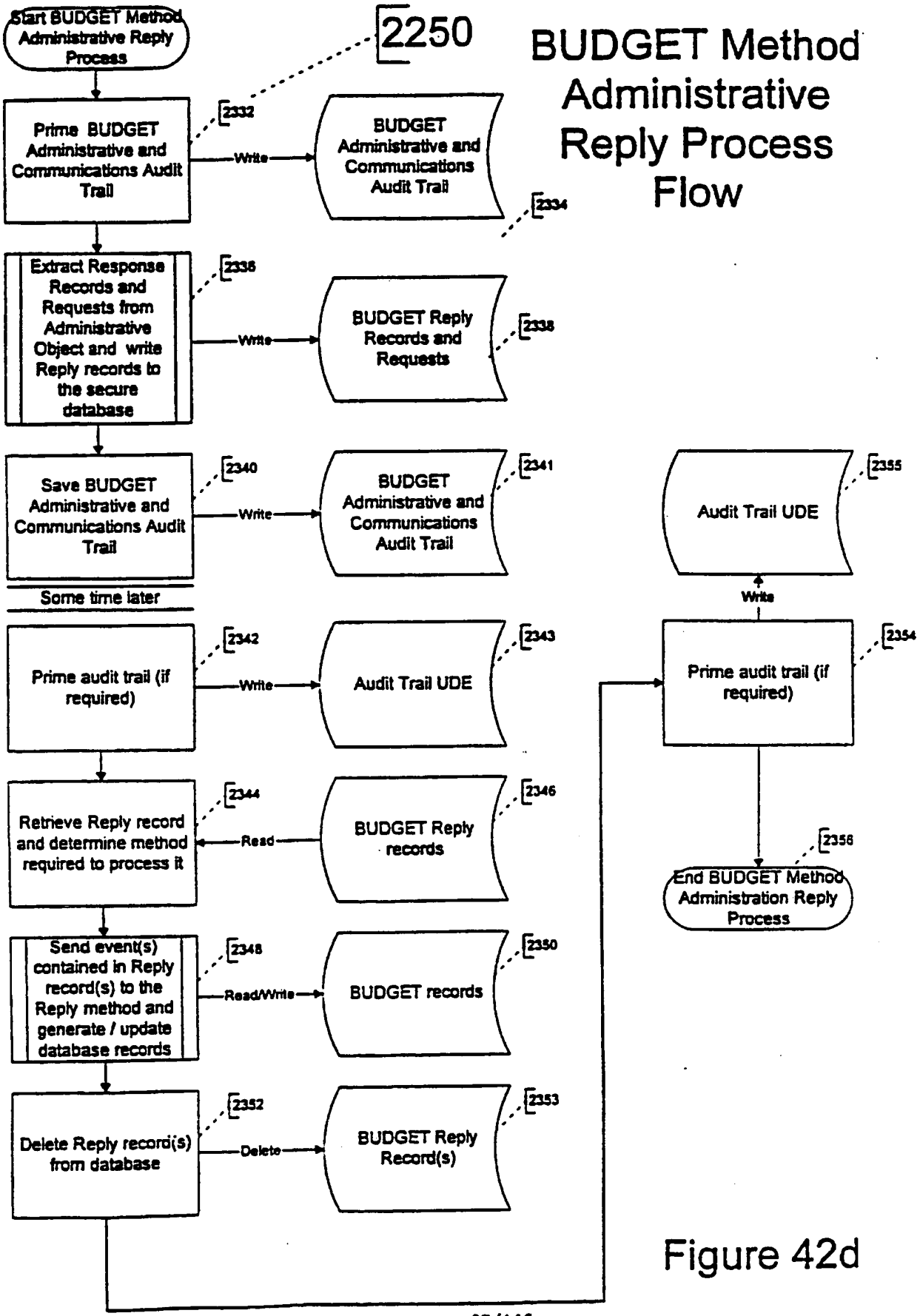
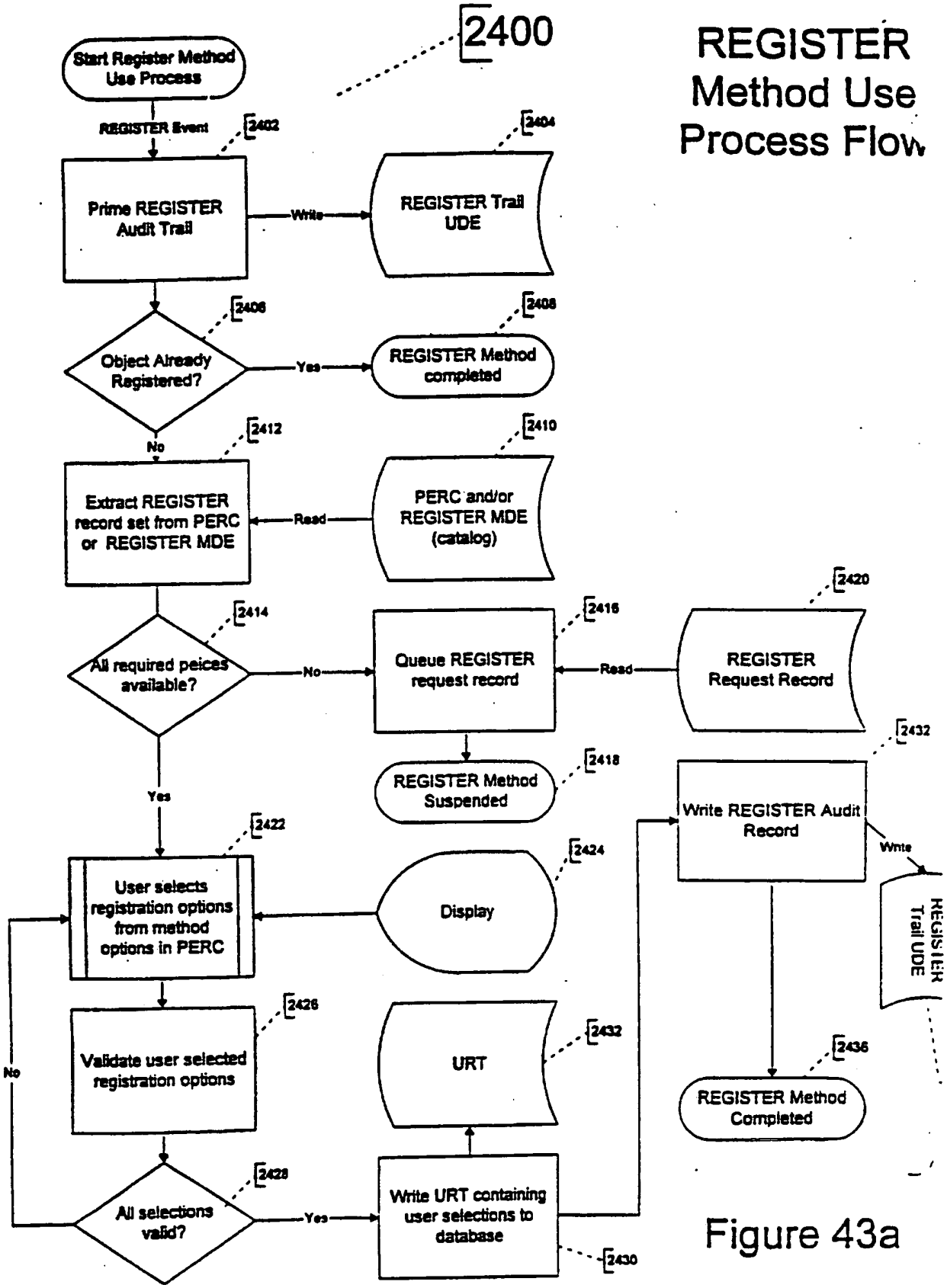

Start BUDGET Method Administrative Reply Process
2250
BUDGET Method Administrative Reply Process Flow
Prime BUDGET Administrative and Communications Audit Trail
2332
Write
BUDGET Administrative and Communications Audit Trail
2334
Extract Response Records and Requests from Administrative Object and write Reply records to the secure database
2336
Write
BUDGET Reply Records and Requests
2338
Save BUDGET Administrative and Communications Audit Trail
2340
Write
BUDGET Administrative and Communications Audit Trail
2341
Some time later
Prime audit trail (if required)
2342
Write
Audit Trail UDE
2343
Retrieve Reply record and determine method required to process it
2344
Read
BUDGET Reply records
2346
Send event(s) contained in Reply record(s) to the Reply method and generate / update database records
2348
Read/Write
BUDGET records
2350
Delete Reply record(s) from database
2352
Delete
BUDGET Reply Record(s)
2353
Audit Trail UDE
2355
Write
Prime audit trail (if required)
2354
2356
End BUDGET Method Administration Reply Process

Figure 42d



REGISTER Method Use Process Flow

Figure 43a

REGISTER Method Administrative Request Process Flow

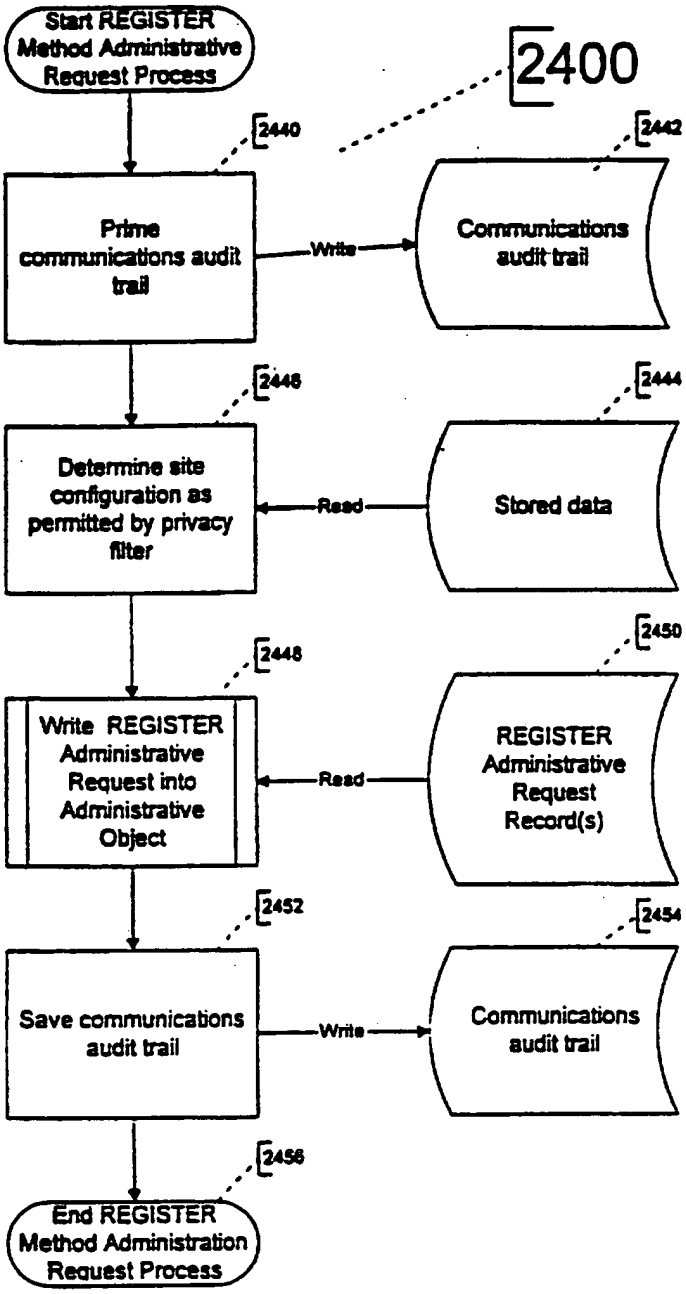
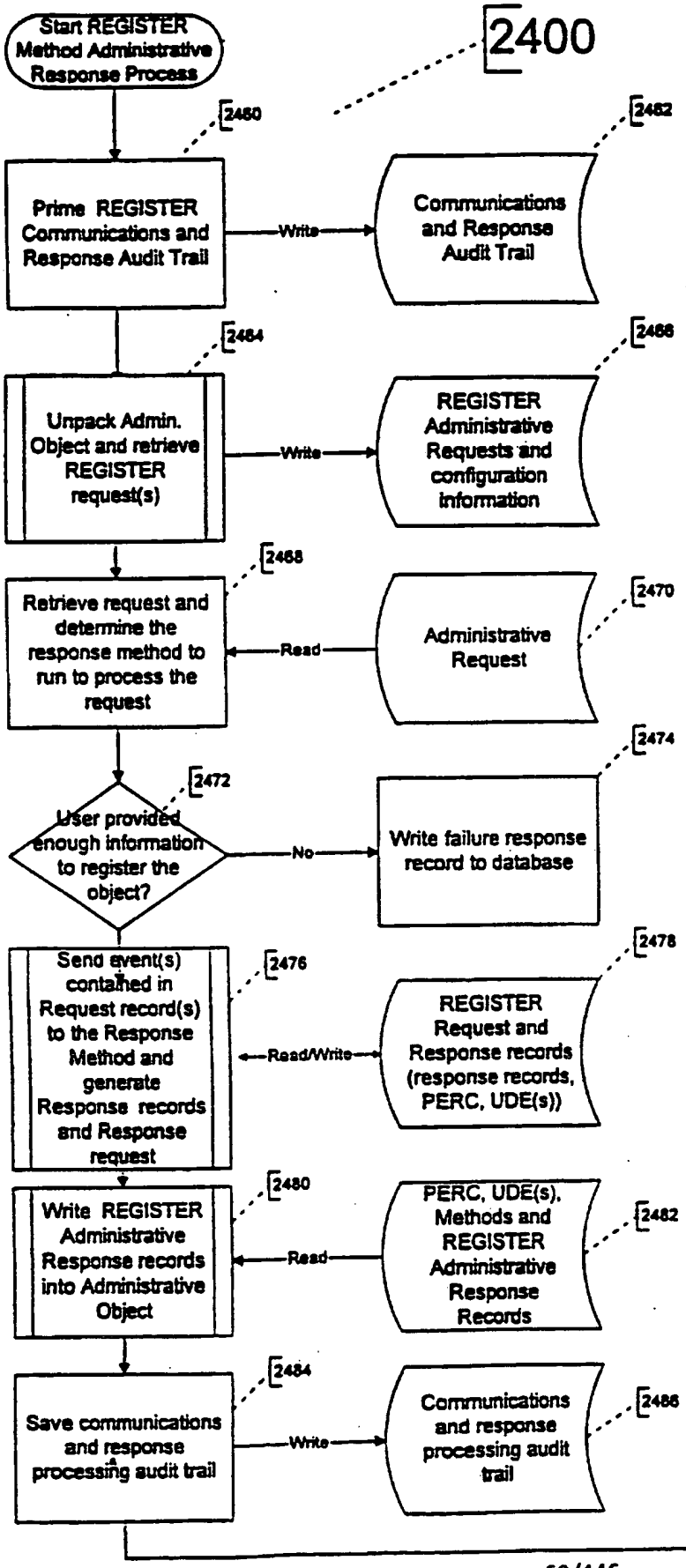


Figure 43b



REGISTER Method Administrative Response Process Flow

Figure 43c

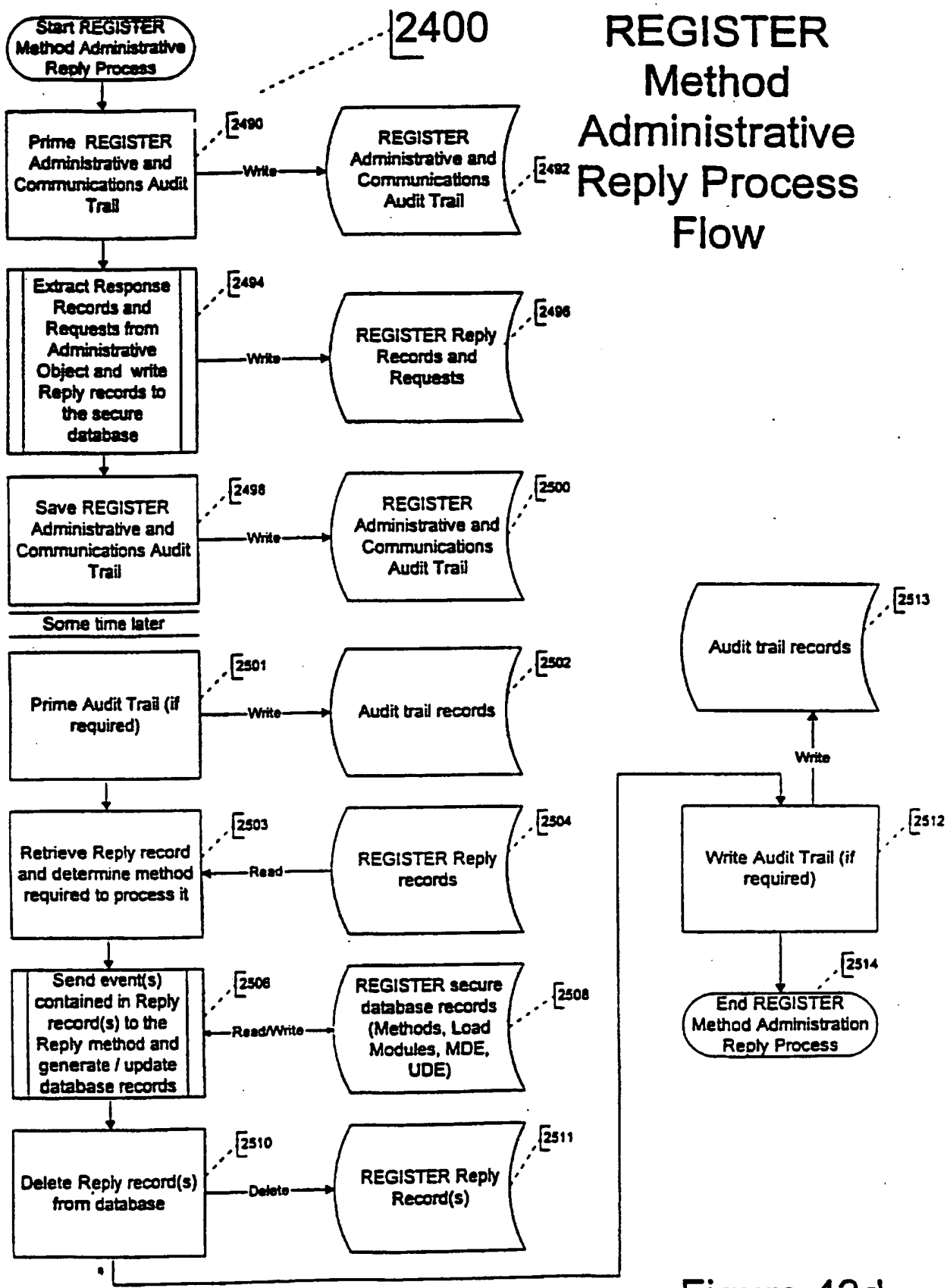
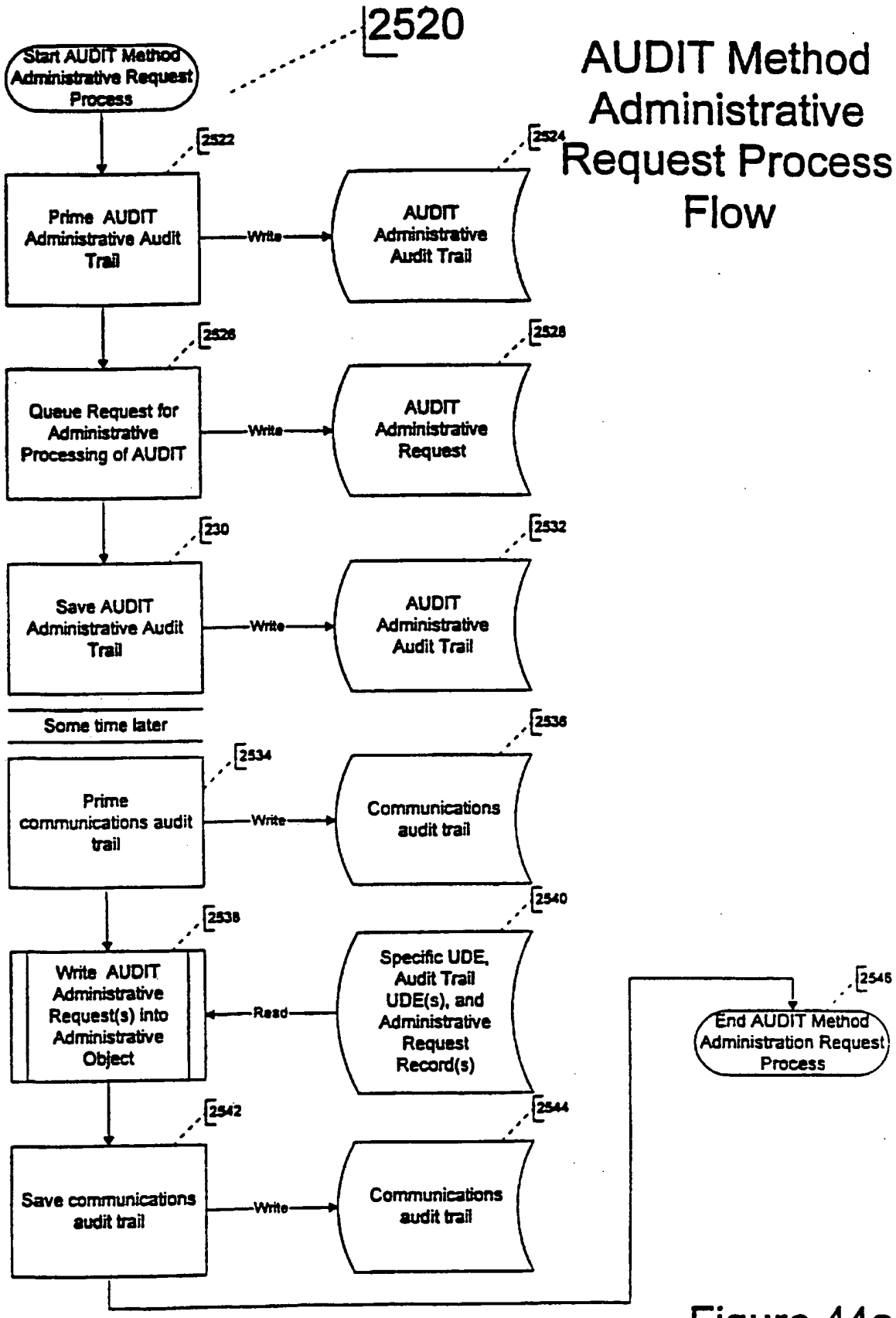

2400
REGISTER Method Administrative Reply Process Flow
Start REGISTER Method Administrative Reply Process
Prime REGISTER Administrative and Communications Audit Trail
2490
Write
REGISTER Administrative and Communications Audit Trail
2492
Extract Response Records and Requests from Administrative Object and write Reply records to the secure database
2494
Write
REGISTER Reply Records and Requests
2496
Save REGISTER Administrative and Communications Audit Trail
2498
Write
REGISTER Administrative and Communications Audit Trail
2500
Some time later
Prime Audit Trail (if required)
2501
Write
Audit trail records
2502
Retrieve Reply record and determine method required to process it
2503
Read
REGISTER Reply records
2504
Send event(s) contained in Reply record(s) to the Reply method and generate / update database records
2506
Read/Write
REGISTER secure database records (Methods, Load Modules, MDE, UDE)
2508
Delete Reply record(s) from database
2510
Delete
REGISTER Reply Record(s)
2511
Audit trail records
2513
Write
Write Audit Trail (if required)
2512
2514
End REGISTER Method Administration Reply Process

Figure 43d



AUDIT Method Administrative Request Process Flow

Figure 44a

AUDIT Method Administrative Response Process Flow

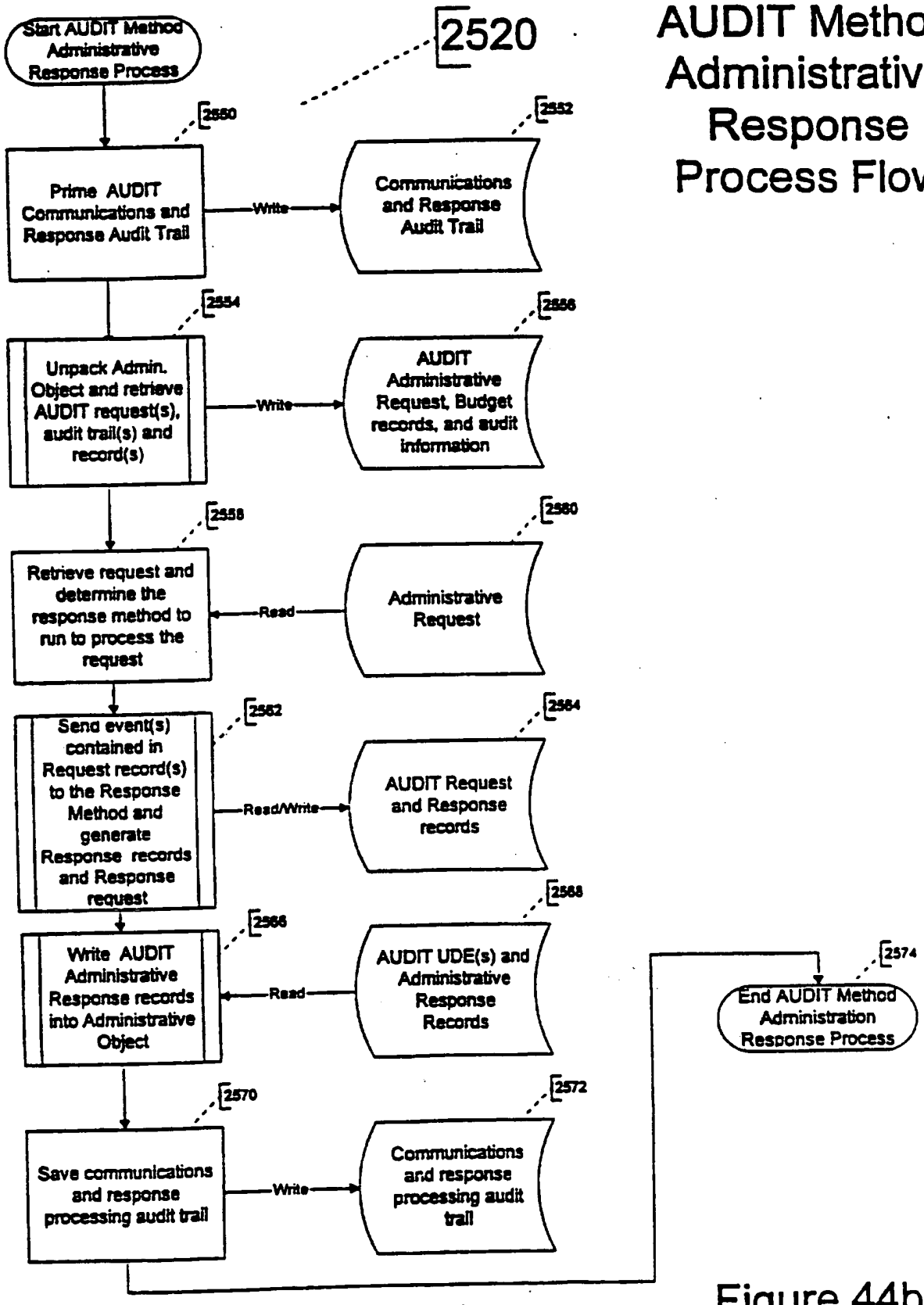


Figure 44b

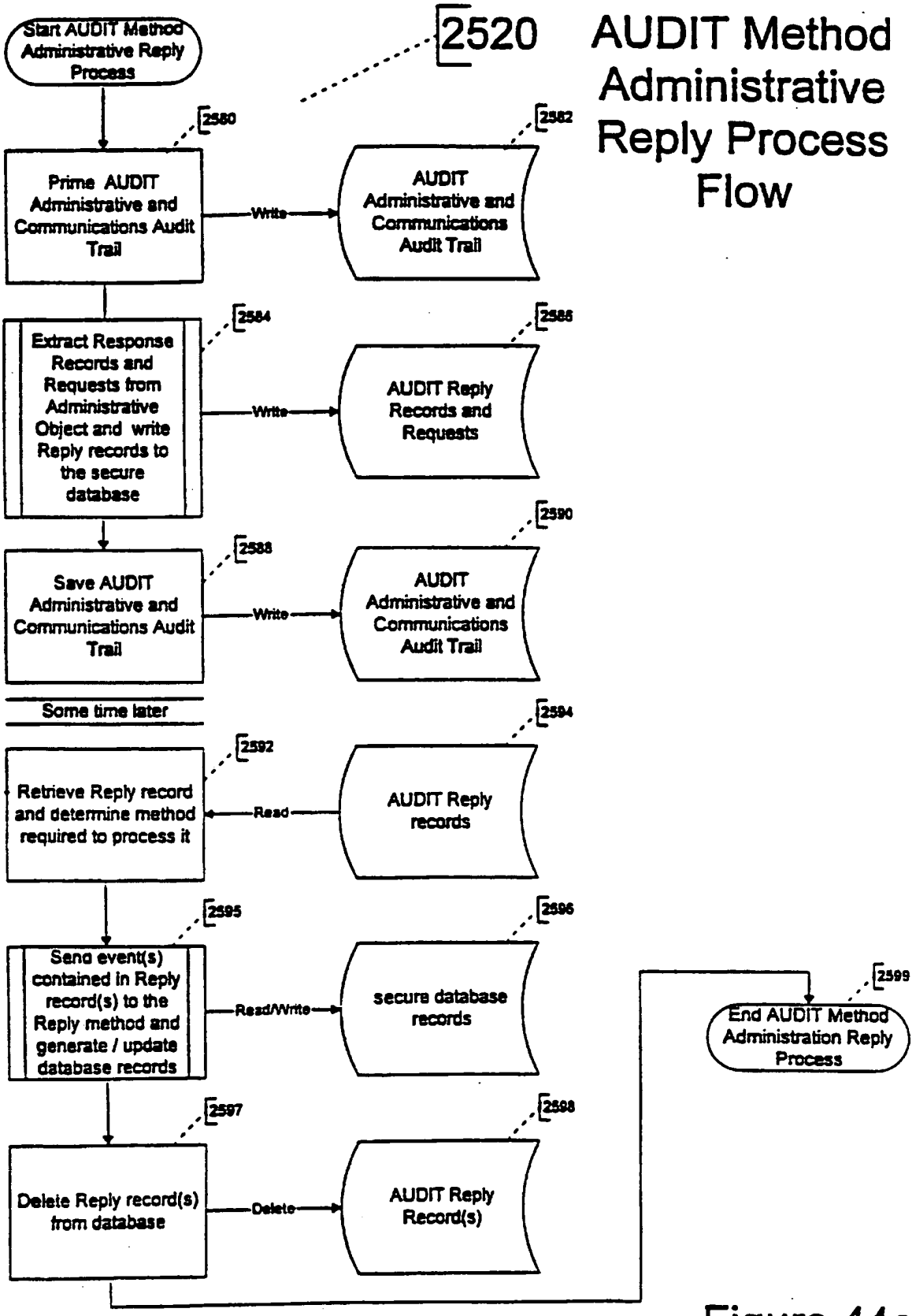

2520
AUDIT Method Administrative Reply Process Flow
Start AUDIT Method Administrative Reply Process
2580
Prime AUDIT Administrative and Communications Audit Trail
Write
2582
AUDIT Administrative and Communications Audit Trail
2584
Extract Response Records and Requests from Administrative Object and write Reply records to the secure database
Write
2586
AUDIT Reply Records and Requests
2588
Save AUDIT Administrative and Communications Audit Trail
Write
2590
AUDIT Administrative and Communications Audit Trail
Some time later
2592
Retrieve Reply record and determine method required to process it
Read
2594
AUDIT Reply records
2595
Send event(s) contained in Reply record(s) to the Reply method and generate / update database records
Read/Write
2596
secure database records
2597
Delete Reply record(s) from database
Delete
2598
AUDIT Reply Record(s)
2599
End AUDIT Method Administration Reply Process

Figure 44c

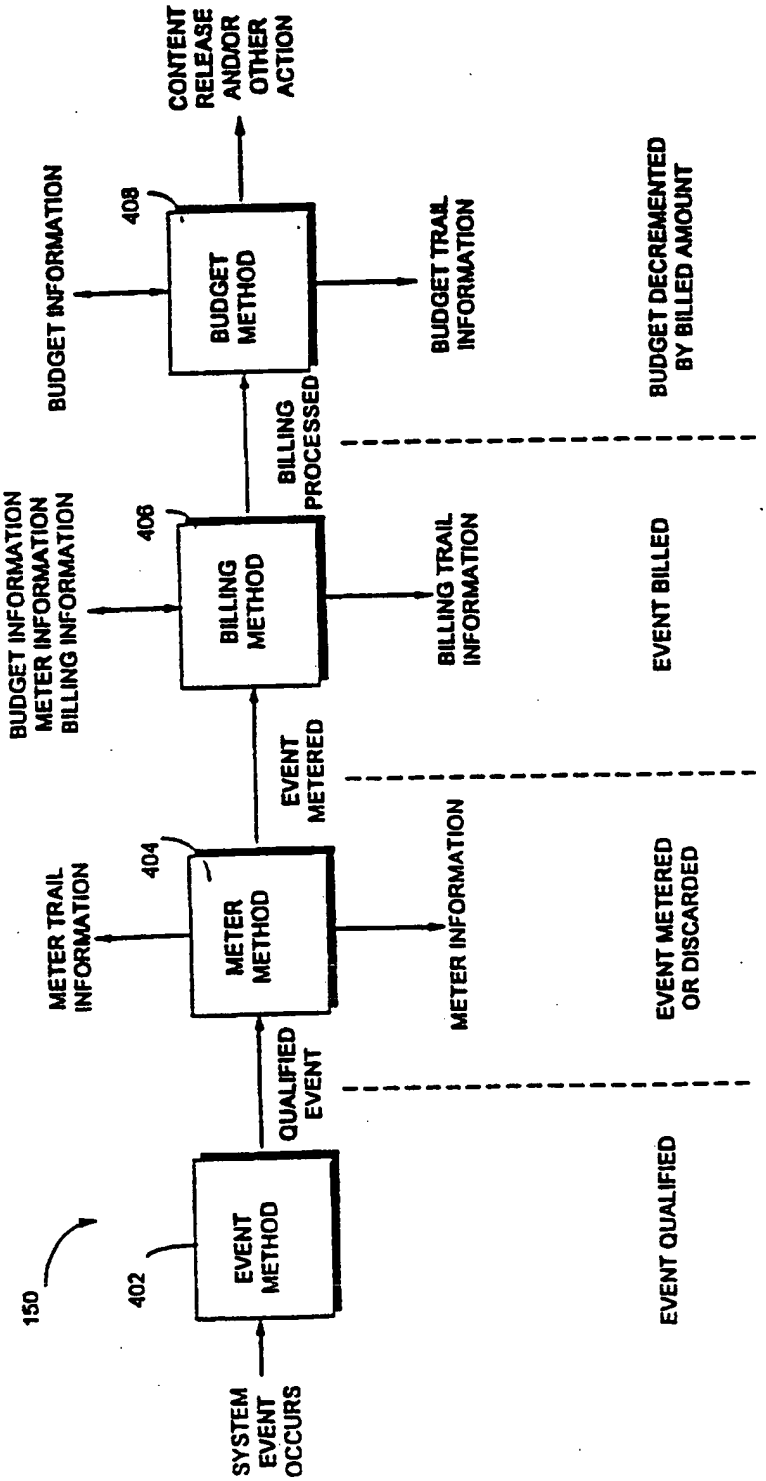
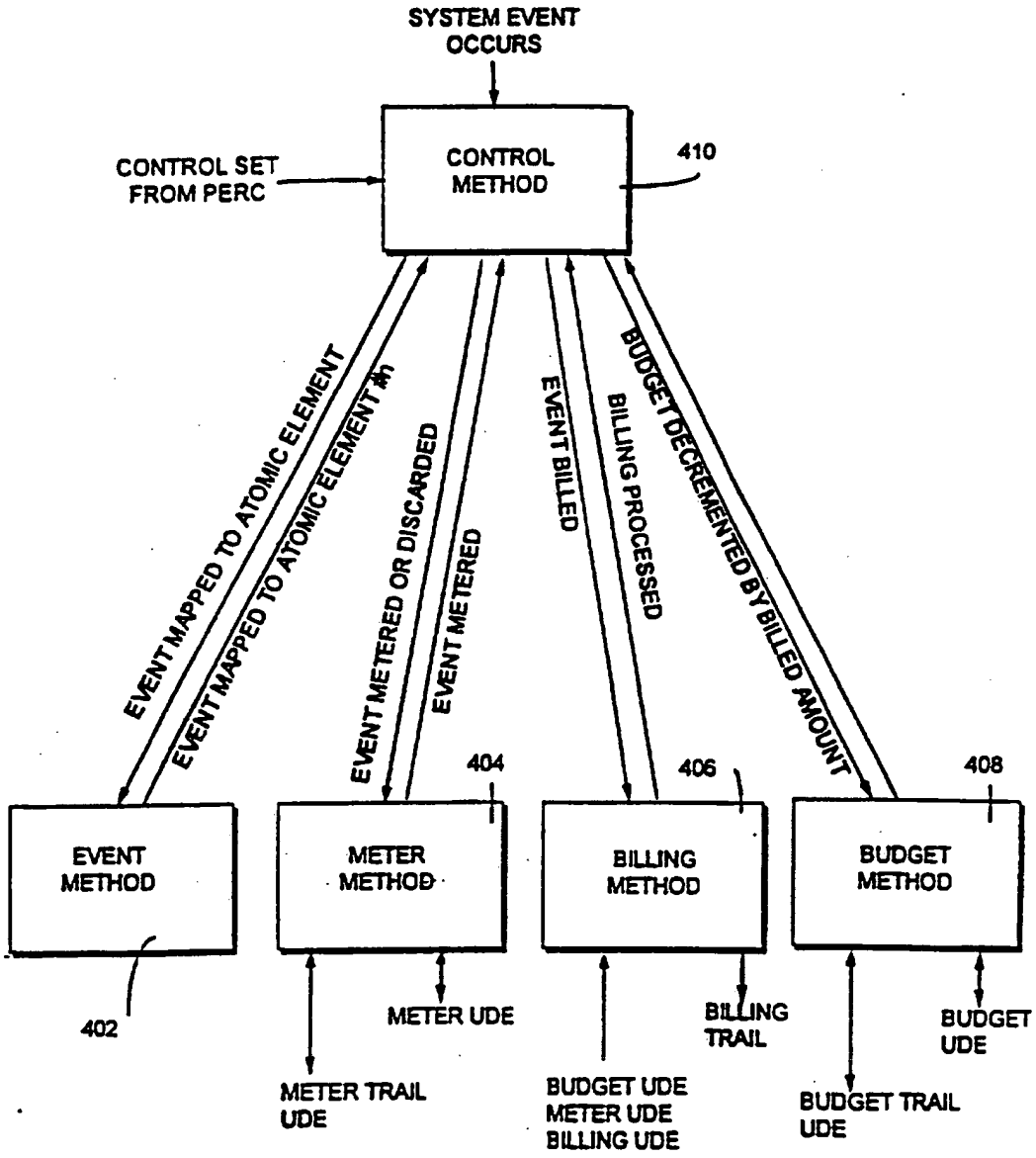

150
402
EVENT METHOD
404
METER METHOD
406
BILLING METHOD
408
BUDGET METHOD
SYSTEM EVENT OCCURS
QUALIFIED EVENT
EVENT METERED
BILLING PROCESSED
METER TRAIL INFORMATION
METER INFORMATION
BILLING TRAIL INFORMATION
BUDGET TRAIL INFORMATION
BUDGET INFORMATION
METER INFORMATION
BILLING INFORMATION
CONTENT RELEASE AND/OR OTHER ACTION
EVENT QUALIFIED
EVENT METERED OR DISCARDED
EVENT BILLED
BUDGET DECREMENTED BY BILLED AMOUNT

FIG. 45

FIG. 46


SYSTEM EVENT OCCURS
CONTROL SET FROM PERC
CONTROL METHOD
410
EVENT MAPPED TO ATOMIC ELEMENT
EVENT MAPPED TO ATOMIC ELEMENT #1
EVENT METERED OR DISCARDED
EVENT METERED
EVENT BILLED
BILLING PROCESSED
BUDGET DECREMENTED BY BILLED AMOUNT
404
406
408
EVENT METHOD
METER METHOD
BILLING METHOD
BUDGET METHOD
402
METER UDE
METER TRAIL UDE
BUDGET UDE
METER UDE
BILLING UDE
BILLING TRAIL
BUDGET UDE
BUDGET TRAIL UDE

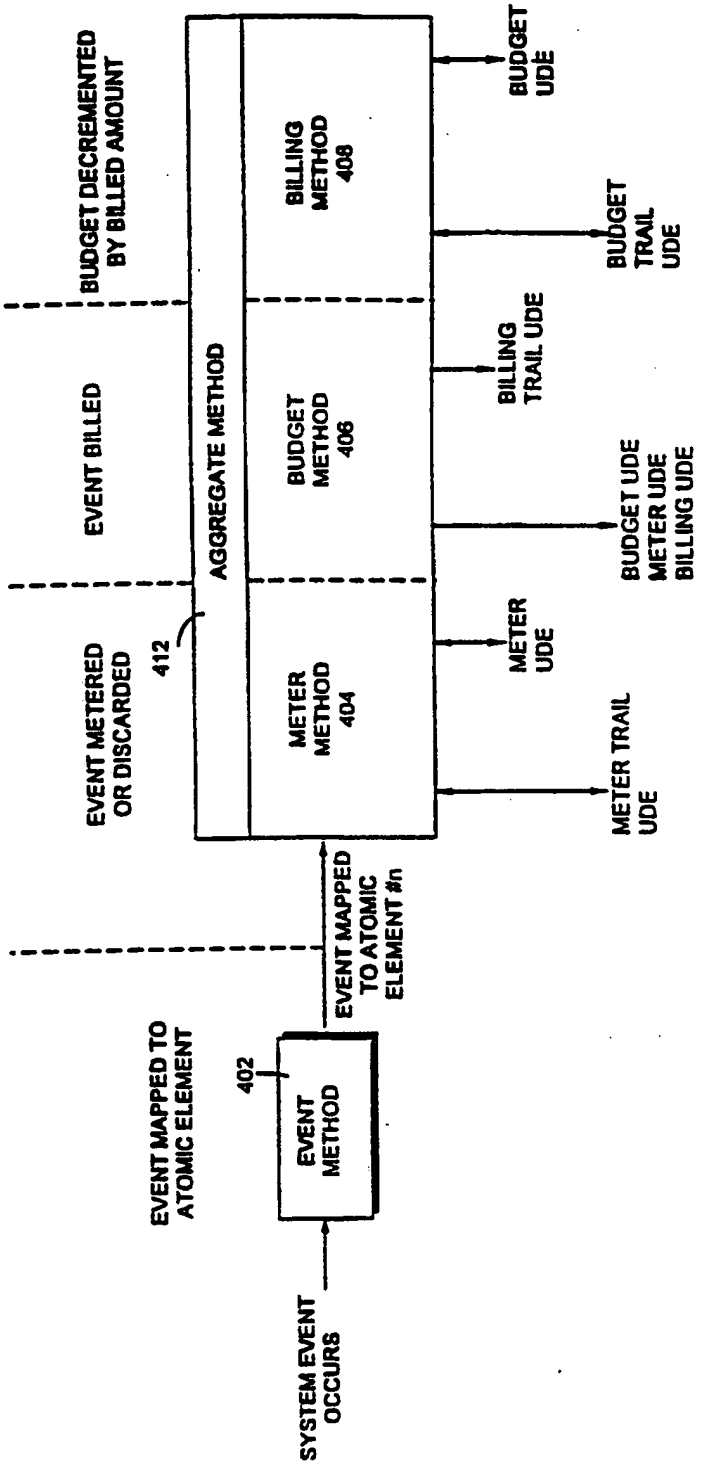

SYSTEM EVENT OCCURS
EVENT MAPPED TO ATOMIC ELEMENT
402
EVENT METHOD
EVENT MAPPED TO ATOMIC ELEMENT #n
412
AGGREGATE METHOD
METER METHOD 404
BUDGET METHOD 406
BILLING METHOD 408
EVENT METERED OR DISCARDED
EVENT BILLED
BUDGET DECREMENTED BY BILLED AMOUNT
METER UDE
METER TRAIL UDE
BILLING TRAIL UDE
BUDGET UDE METER UDE BILLING UDE
BUDGET TRAIL UDE
BUDGET UDE

FIG. 47

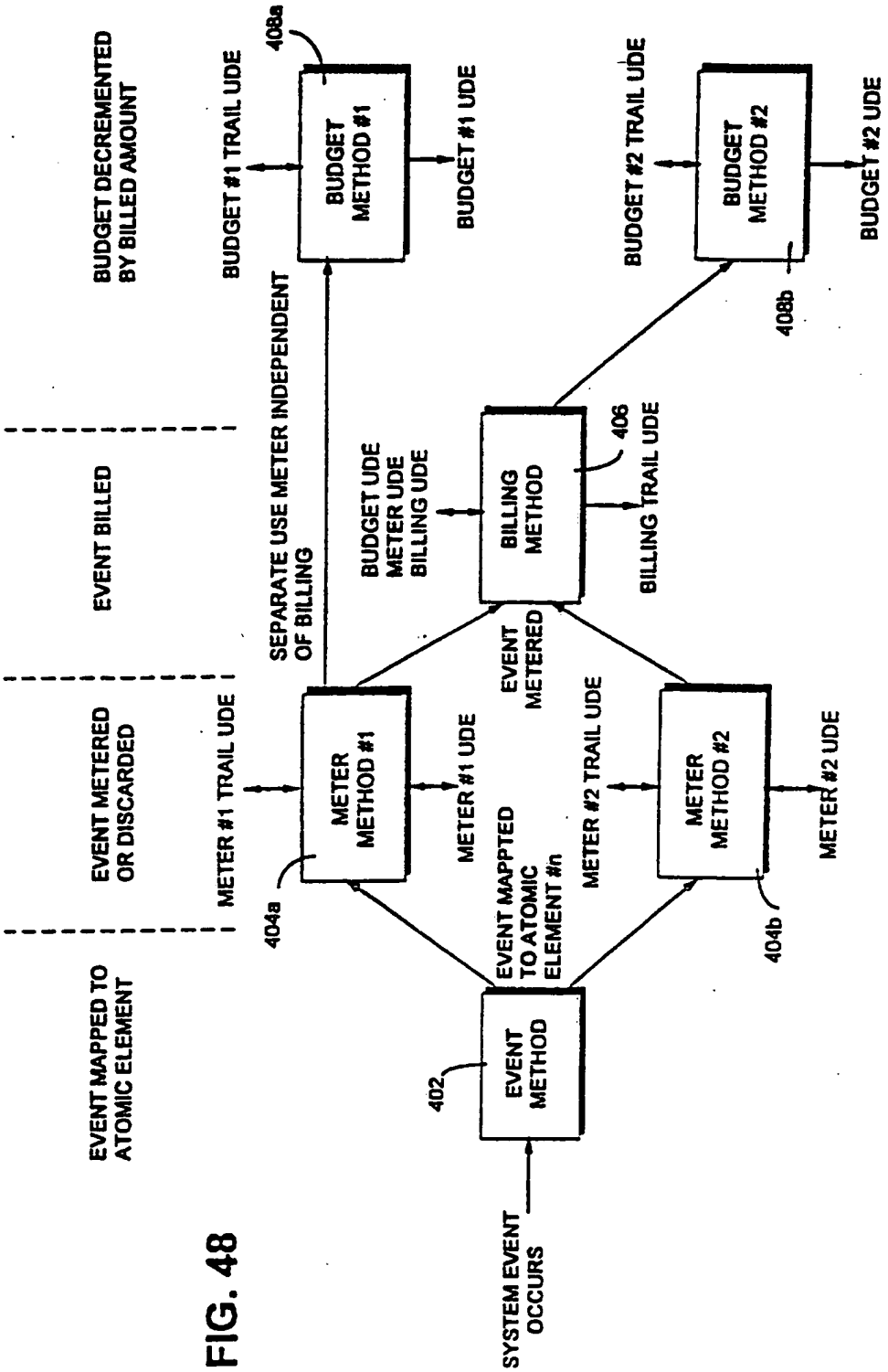

EVENT MAPPED TO ATOMIC ELEMENT
EVENT METERED OR DISCARDED
EVENT BILLED
BUDGET DECREMENTED BY BILLED AMOUNT
SYSTEM EVENT OCCURS
EVENT METHOD
402
EVENT MAPPED TO ATOMIC ELEMENT #n
METER METHOD #1
404a
METER #1 TRAIL UDE
METER #1 UDE
METER METHOD #2
404b
METER #2 TRAIL UDE
METER #2 UDE
EVENT METERED
SEPARATE USE METER INDEPENDENT OF BILLING
BUDGET UDE
METER UDE
BILLING UDE
BILLING METHOD
406
BILLING TRAIL UDE
BUDGET METHOD #1
408a
BUDGET #1 TRAIL UDE
BUDGET #1 UDE
BUDGET METHOD #2
408b
BUDGET #2 TRAIL UDE
BUDGET #2 UDE

FIG. 48

OPEN Method Use Process Flow

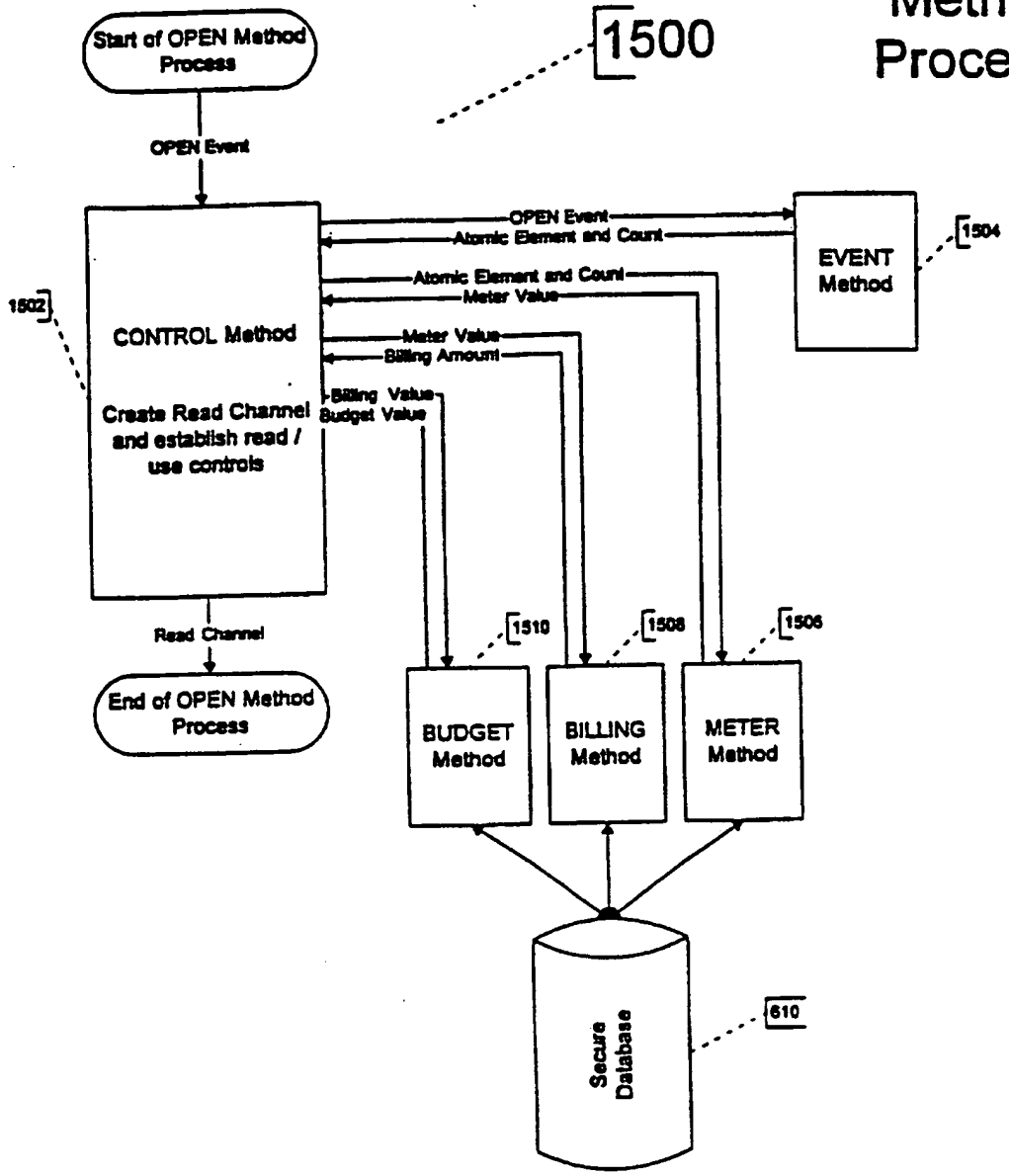


Figure 49

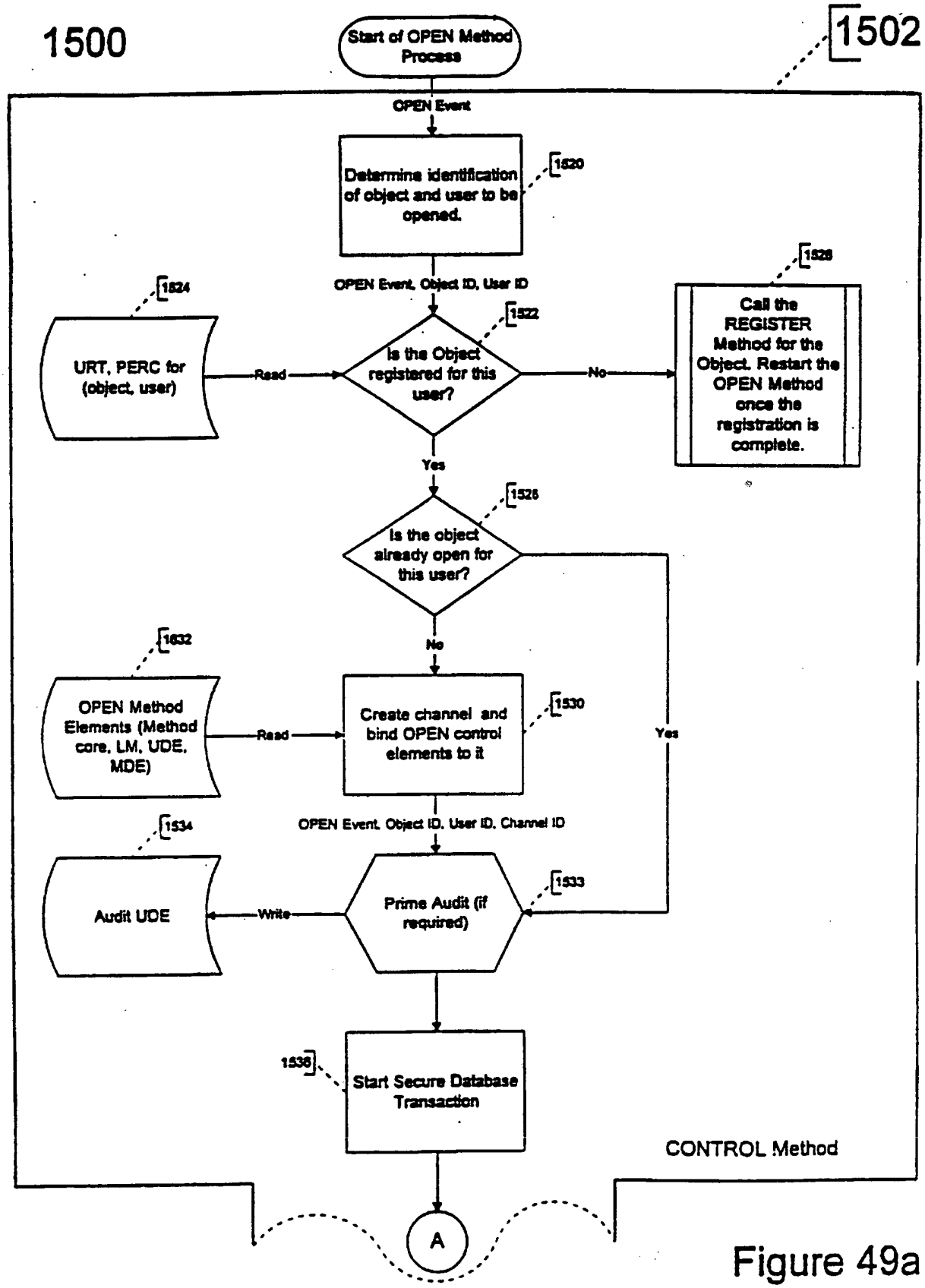

1500
Start of OPEN Method Process
1502
OPEN Event
Determine identification of object and user to be opened.
1520
OPEN Event, Object ID, User ID
1524
URT, PERC for (object, user)
Read
1522
Is the Object registered for this user?
No
1528
Call the REGISTER Method for the Object. Restart the OPEN Method once the registration is complete.
Yes
1526
Is the object already open for this user?
Yes
No
1532
OPEN Method Elements (Method core, LM, UDE, MDE)
Read
Create channel and bind OPEN control elements to it
1530
OPEN Event, Object ID, User ID, Channel ID
1534
Audit UDE
Write
Prime Audit (if required)
1533
1536
Start Secure Database Transaction
CONTROL Method
A

Figure 49a

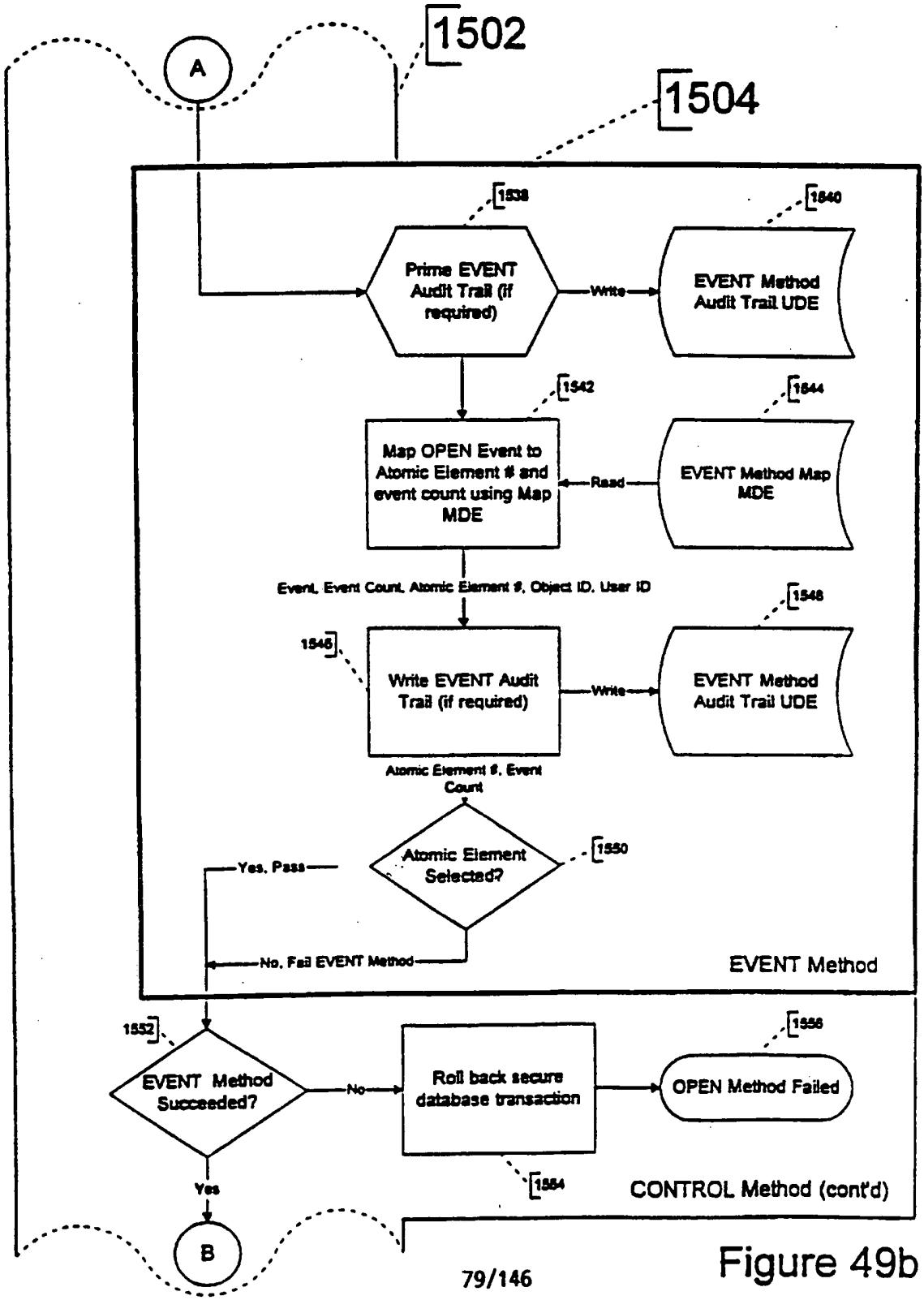

1502
1504
A
1538
Prime EVENT Audit Trail (if required)
Write
1540
EVENT Method Audit Trail UDE
1542
Map OPEN Event to Atomic Element # and event count using Map MDE
Read
1544
EVENT Method Map MDE
Event, Event Count, Atomic Element #, Object ID, User ID
1546
Write EVENT Audit Trail (if required)
Write
1548
EVENT Method Audit Trail UDE
Atomic Element #, Event Count
Atomic Element Selected?
1550
Yes, Pass
No, Fail EVENT Method
EVENT Method
1552
EVENT Method Succeeded?
No
Roll back secure database transaction
1554
1556
OPEN Method Failed
Yes
CONTROL Method (cont'd)
B

Figure 49b

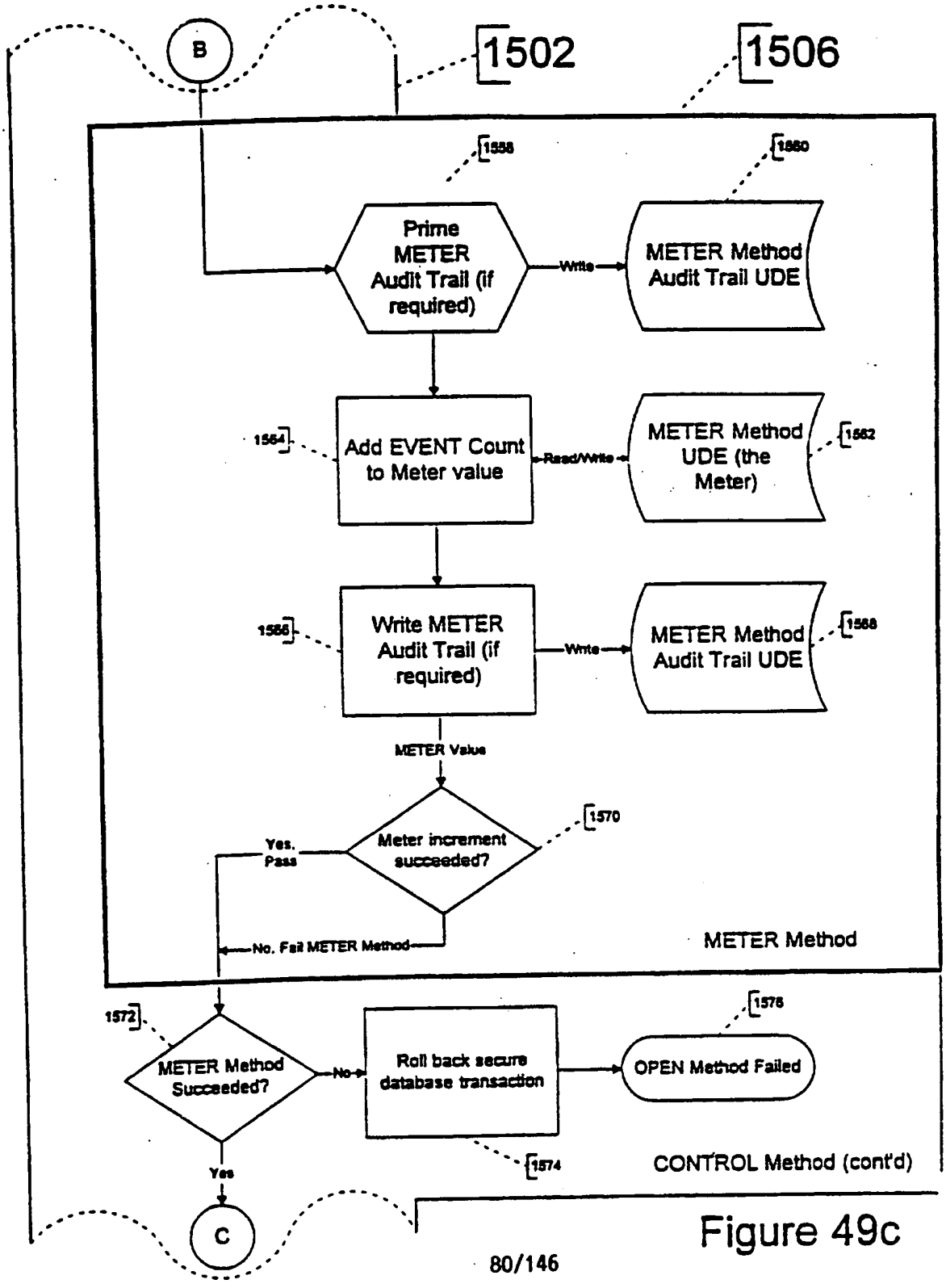

B
1502
1506
1558
1560
Prime METER Audit Trail (if required)
Write
METER Method Audit Trail UDE
1564
Add EVENT Count to Meter value
Read/Write
METER Method UDE (the Meter)
1562
1566
Write METER Audit Trail (if required)
Write
METER Method Audit Trail UDE
1568
METER Value
1570
Meter increment succeeded?
Yes, Pass
No, Fail METER Method
METER Method
1572
METER Method Succeeded?
No
Roll back secure database transaction
1574
1576
OPEN Method Failed
CONTROL Method (cont'd)
Yes
C

Figure 49c

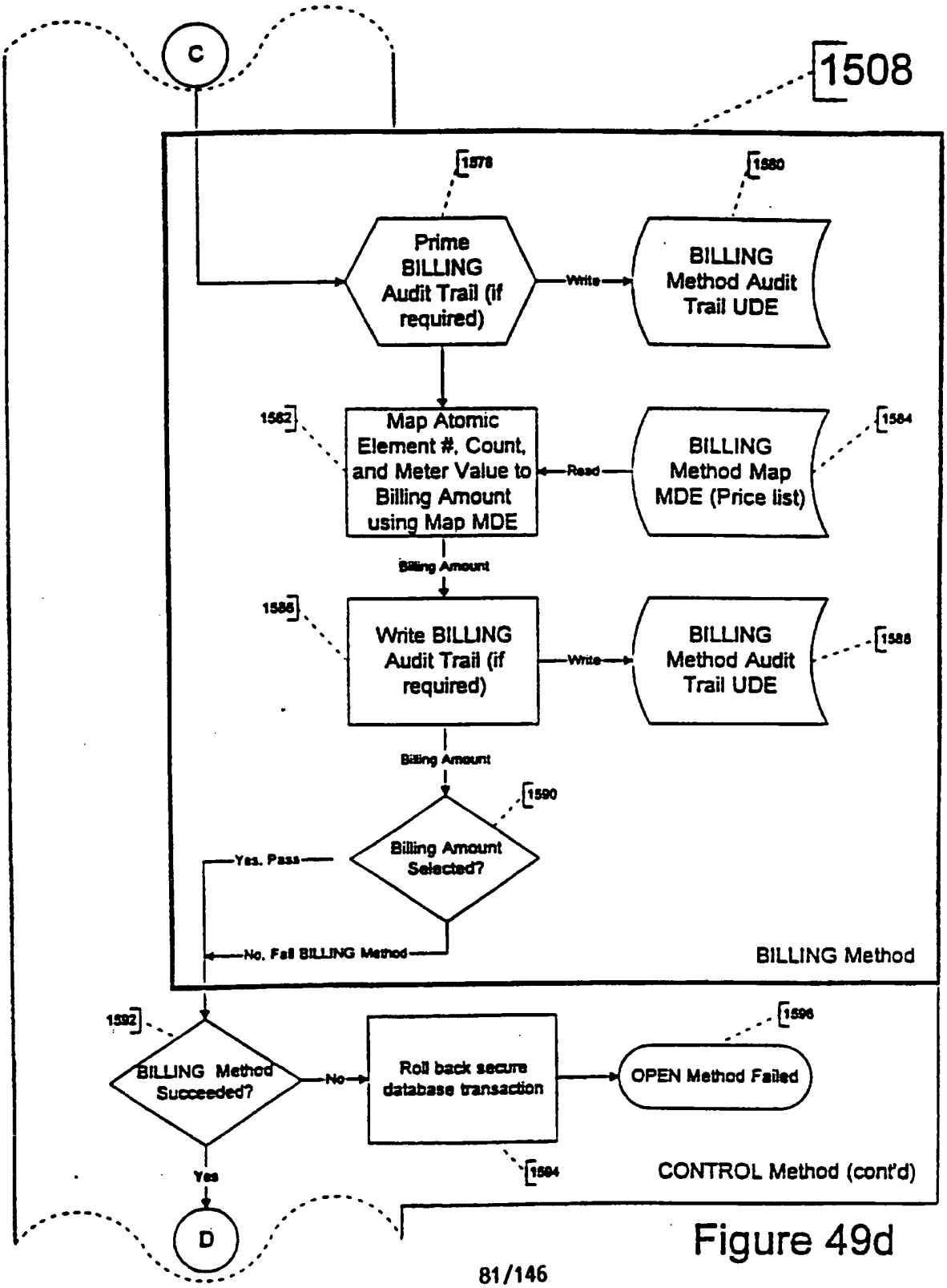

C
1508
1578
Prime BILLING Audit Trail (if required)
Write
1580
BILLING Method Audit Trail UDE
1582
Map Atomic Element #, Count, and Meter Value to Billing Amount using Map MDE
Read
BILLING Method Map MDE (Price list)
1584
Billing Amount
1586
Write BILLING Audit Trail (if required)
Write
BILLING Method Audit Trail UDE
1588
Billing Amount
1590
Billing Amount Selected?
Yes, Pass
No, Fail BILLING Method
BILLING Method
1592
BILLING Method Succeeded?
No
Roll back secure database transaction
1594
OPEN Method Failed
1596
Yes
CONTROL Method (cont'd)
D

Figure 49d

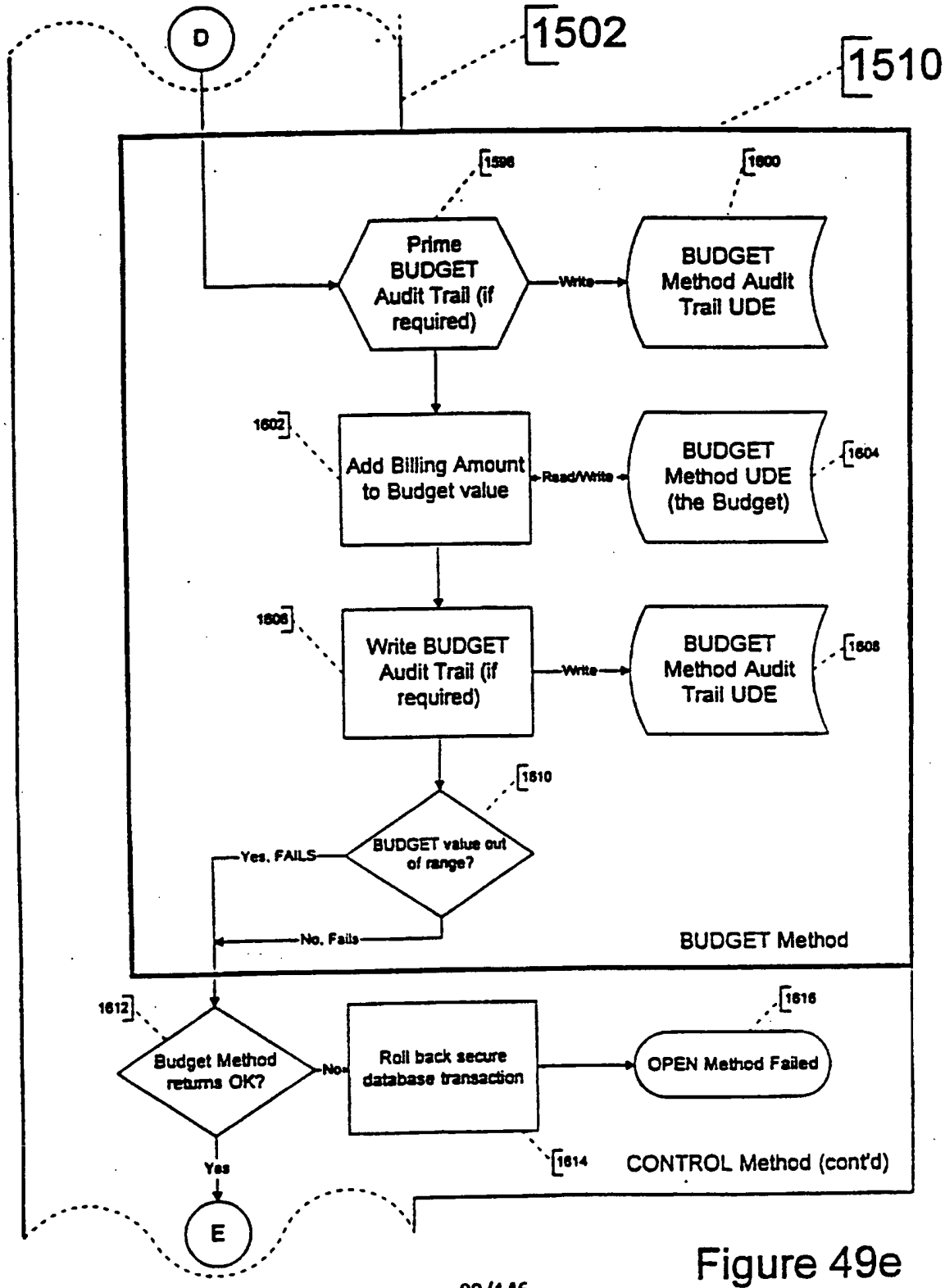

D
1502
1510
1598
1600
Prime BUDGET Audit Trail (if required)
Write
BUDGET Method Audit Trail UDE
1602
Add Billing Amount to Budget value
Read/Write
BUDGET Method UDE (the Budget)
1604
1606
Write BUDGET Audit Trail (if required)
Write
BUDGET Method Audit Trail UDE
1608
1610
BUDGET value out of range?
Yes, FAILS
No, Fails
BUDGET Method
1612
Budget Method returns OK?
No
Roll back secure database transaction
1614
1616
OPEN Method Failed
Yes
CONTROL Method (cont'd)
E

Figure 49e

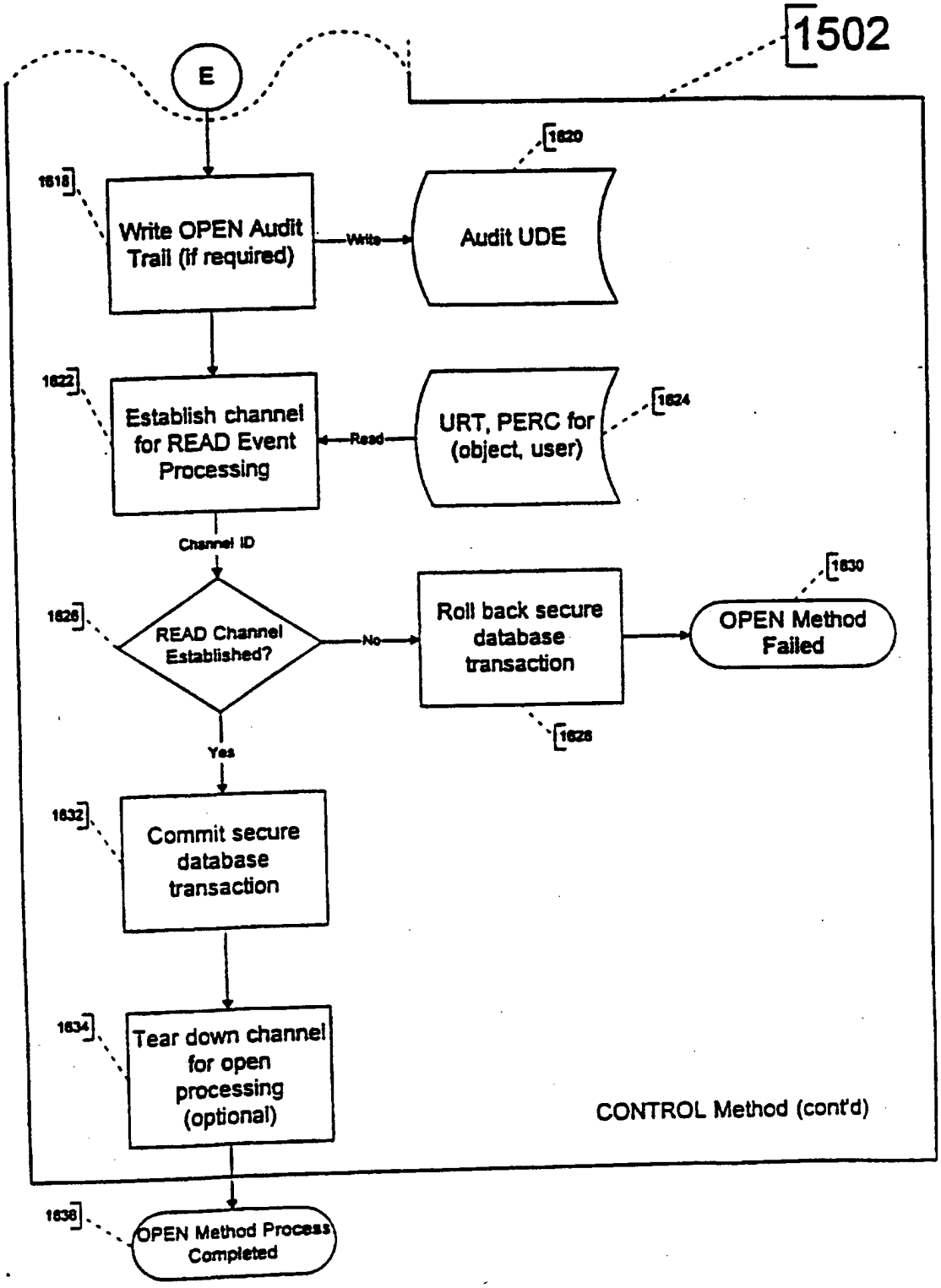

1502
E
1618
Write OPEN Audit Trail (if required)
Write
1620
Audit UDE
1622
Establish channel for READ Event Processing
Read
URT, PERC for (object, user)
1624
Channel ID
1626
READ Channel Established?
No
Roll back secure database transaction
1628
1630
OPEN Method Failed
Yes
1632
Commit secure database transaction
1634
Tear down channel for open processing (optional)
CONTROL Method (cont'd)
1636
OPEN Method Process Completed

Figure 49f

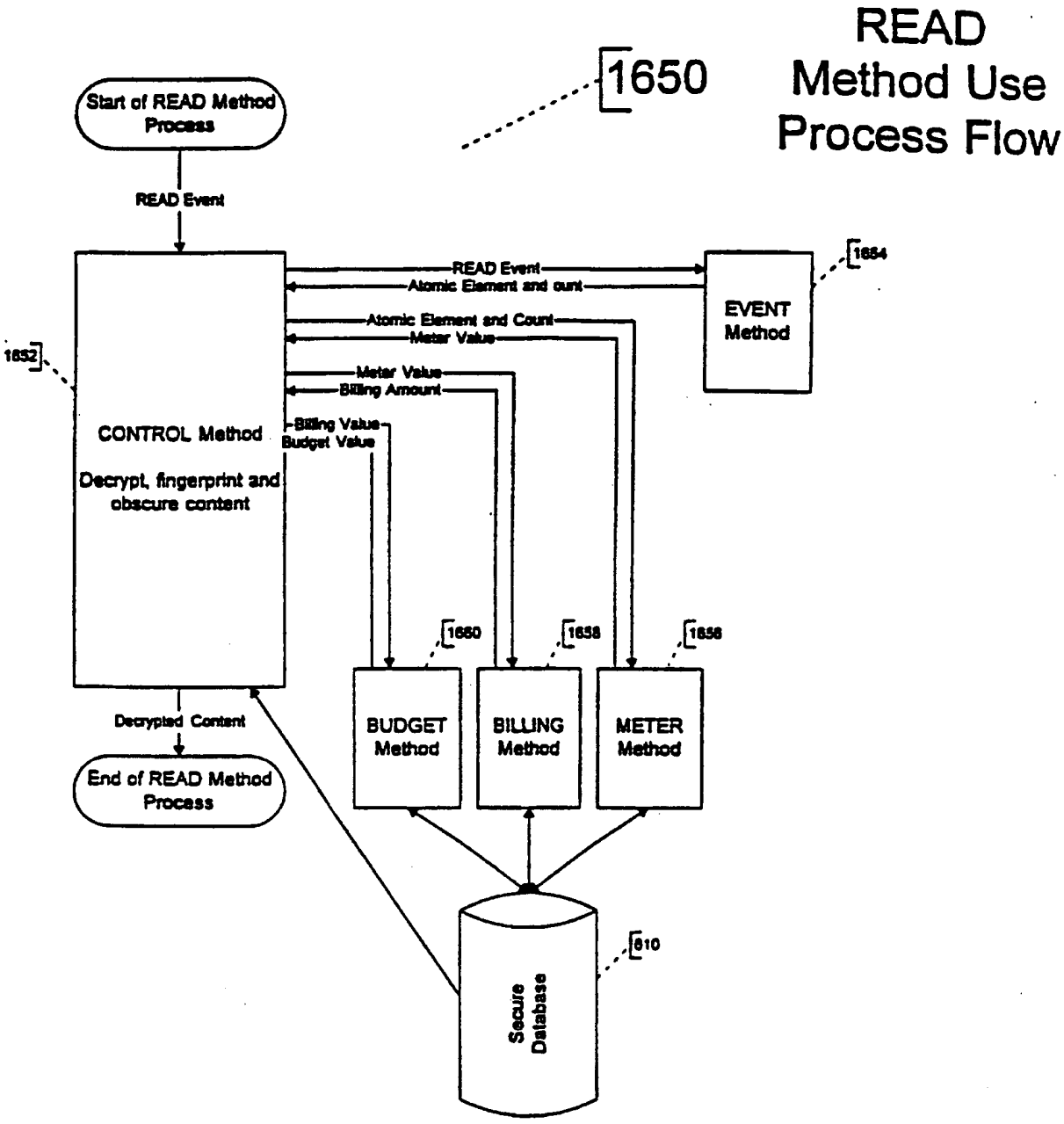

READ
Method Use
Process Flow
1650
Start of READ Method Process
READ Event
1652
CONTROL Method
Decrypt, fingerprint and obscure content
Decrypted Content
End of READ Method Process
READ Event
Atomic Element and ount
Atomic Element and Count
Meter Value
Meter Value
Billing Amount
Billing Value
Budget Value
1654
EVENT Method
1660
1658
1656
BUDGET Method
BILLING Method
METER Method
610
Secure Database

Figure 50

1650

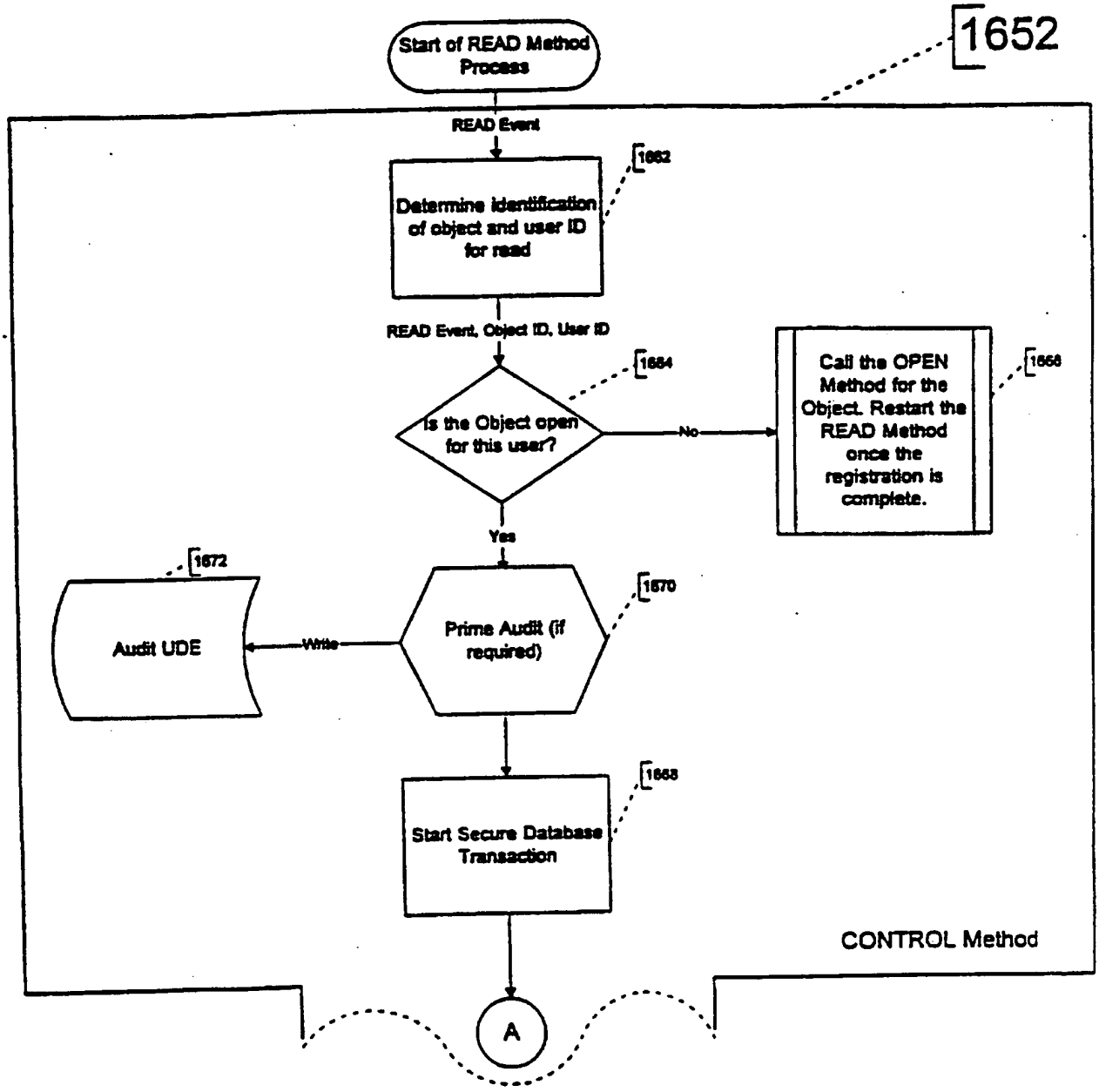


Figure 50a

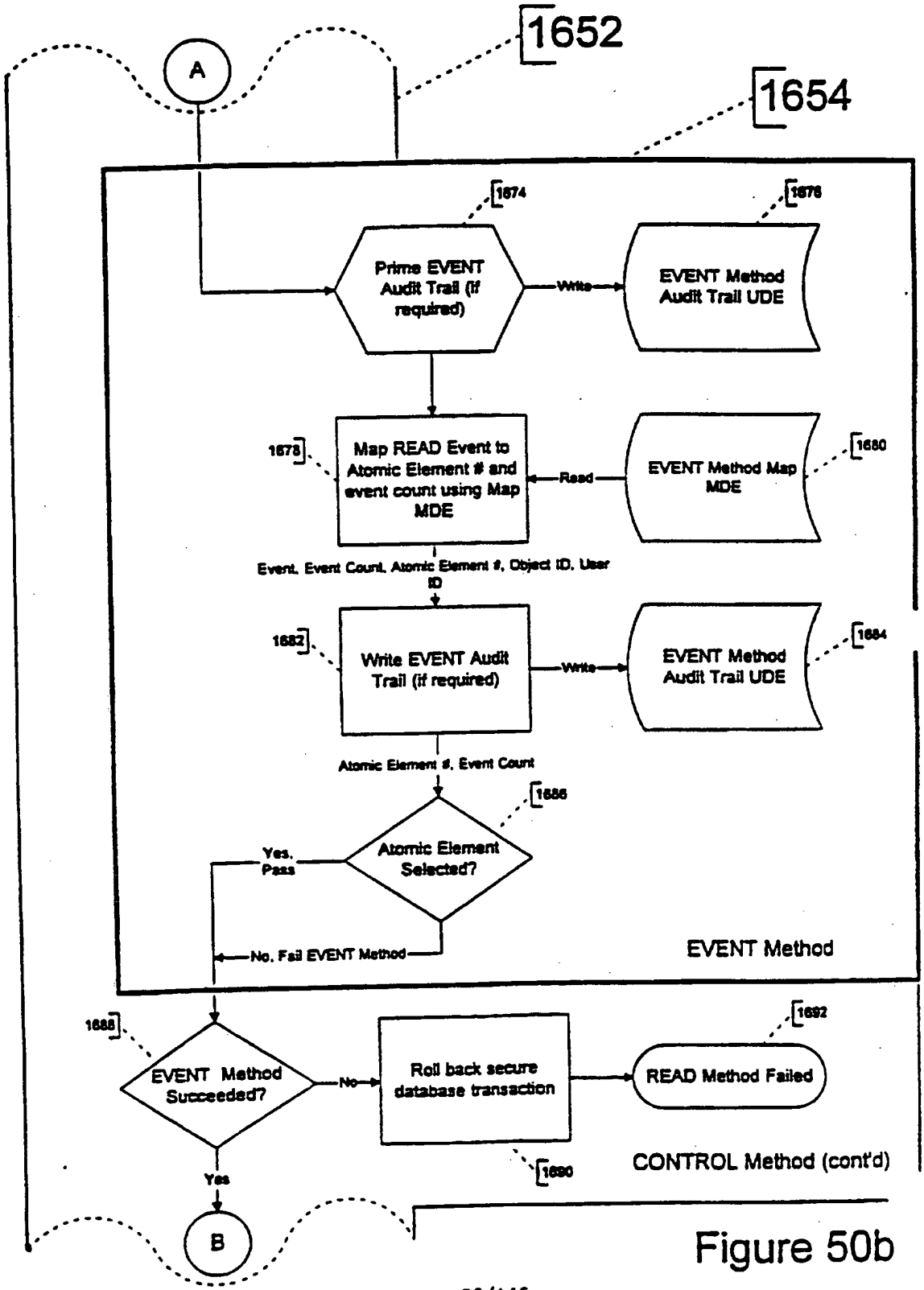

1652
A
1654
1674
Prime EVENT Audit Trail (if required)
Write
1676
EVENT Method Audit Trail UDE
1678
Map READ Event to Atomic Element # and event count using Map MDE
Read
EVENT Method Map MDE
1680
Event, Event Count, Atomic Element #, Object ID, User ID
1682
Write EVENT Audit Trail (if required)
Write
EVENT Method Audit Trail UDE
1684
Atomic Element #, Event Count
1686
Atomic Element Selected?
Yes, Pass
No, Fail EVENT Method
EVENT Method
1688
EVENT Method Succeeded?
No
Roll back secure database transaction
1690
1692
READ Method Failed
CONTROL Method (cont'd)
Yes
B

Figure 50b

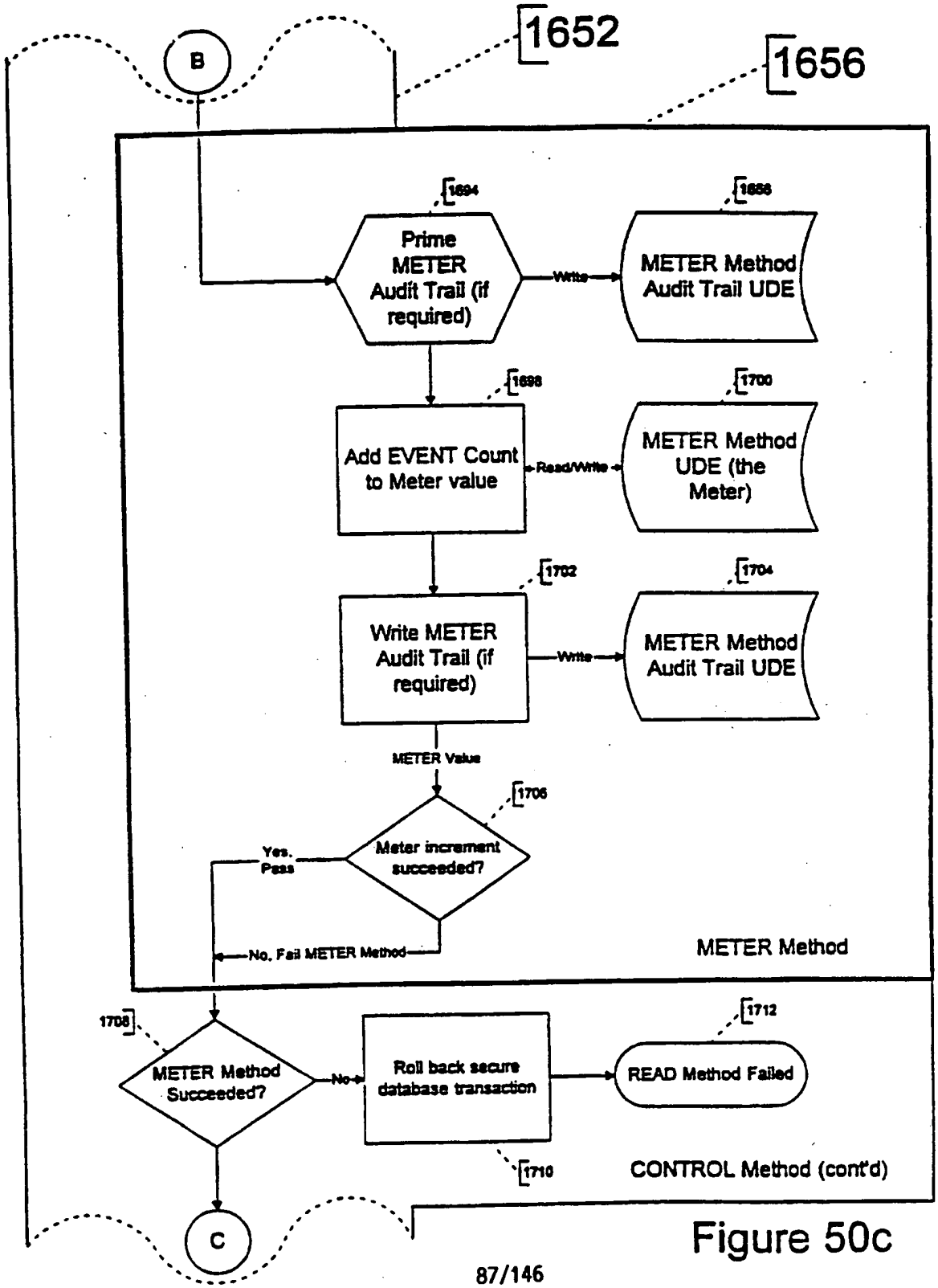

B
1652
1656
1694
Prime METER Audit Trail (if required)
Write
1666
METER Method Audit Trail UDE
1698
Add EVENT Count to Meter value
Read/Write
1700
METER Method UDE (the Meter)
1702
Write METER Audit Trail (if required)
Write
1704
METER Method Audit Trail UDE
METER Value
1706
Meter increment succeeded?
Yes, Pass
No, Fail METER Method
METER Method
1708
METER Method Succeeded?
No
Roll back secure database transaction
1712
READ Method Failed
1710
CONTROL Method (cont'd)
C

Figure 50c

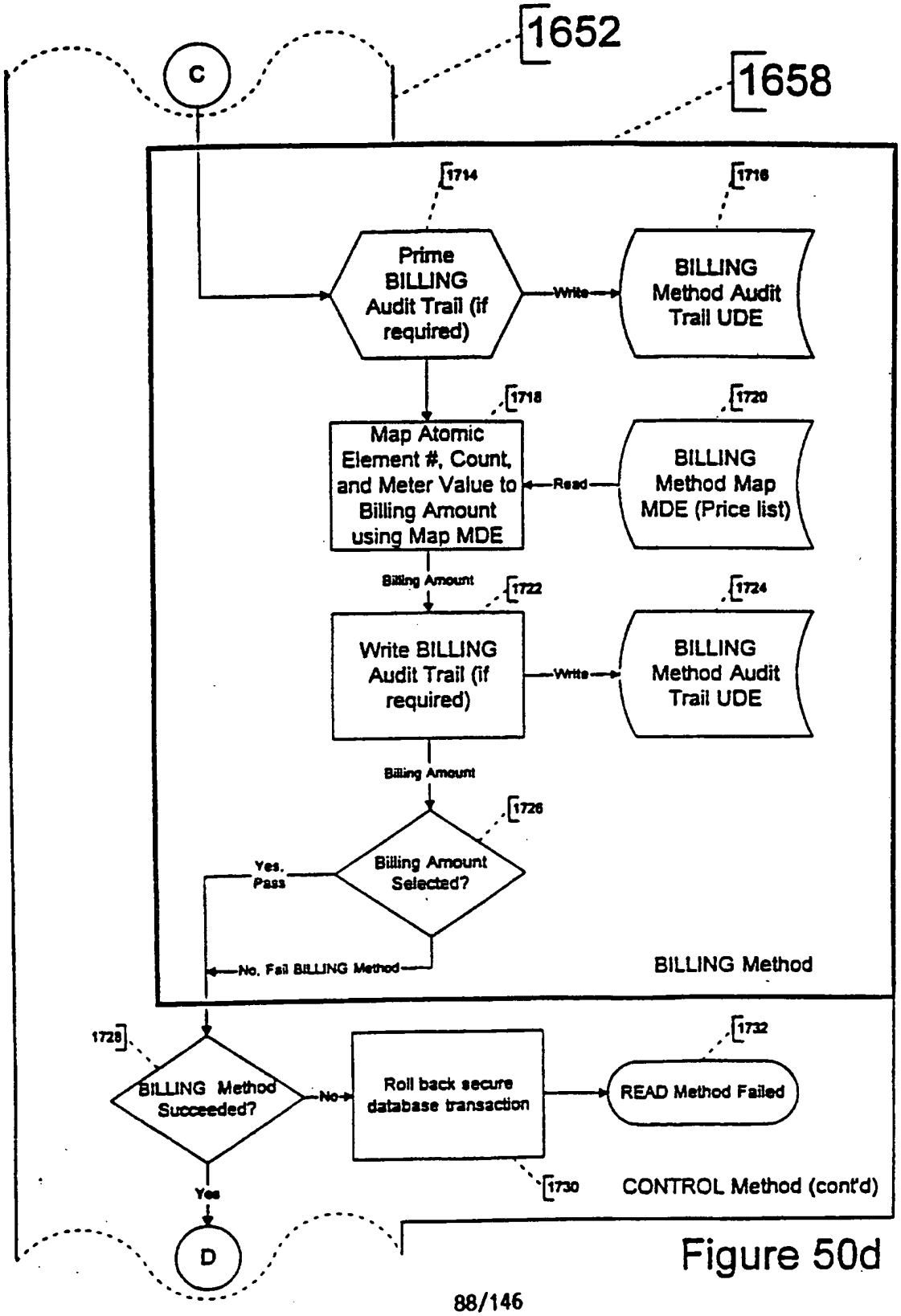

1652
1658
C
1714
1716
Prime BILLING Audit Trail (if required)
Write
BILLING Method Audit Trail UDE
1718
1720
Map Atomic Element #, Count, and Meter Value to Billing Amount using Map MDE
Read
BILLING Method Map MDE (Price list)
Billing Amount
1722
1724
Write BILLING Audit Trail (if required)
Write
BILLING Method Audit Trail UDE
Billing Amount
1726
Billing Amount Selected?
Yes, Pass
No, Fail BILLING Method
BILLING Method
1728
BILLING Method Succeeded?
No
Roll back secure database transaction
1730
1732
READ Method Failed
CONTROL Method (cont'd)
Yes
D

Figure 50d

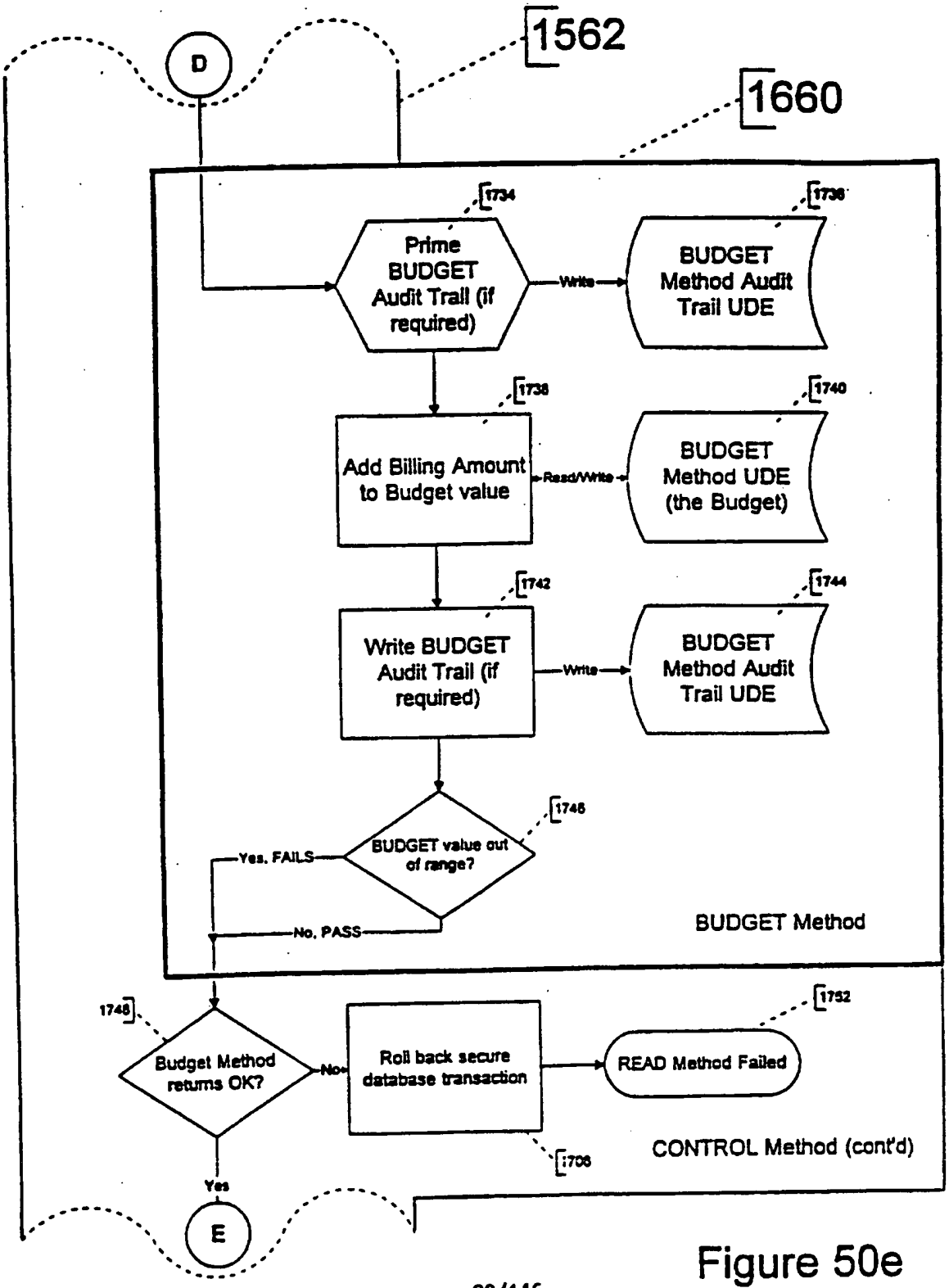

1562
1660
D
1734
Prime BUDGET Audit Trail (if required)
Write
1736
BUDGET Method Audit Trail UDE
1738
Add Billing Amount to Budget value
Read/Write
1740
BUDGET Method UDE (the Budget)
1742
Write BUDGET Audit Trail (if required)
Write
1744
BUDGET Method Audit Trail UDE
1746
BUDGET value out of range?
Yes, FAILS
No, PASS
BUDGET Method
1748
Budget Method returns OK?
No
Roll back secure database transaction
1752
READ Method Failed
1706
CONTROL Method (cont'd)
Yes
E

Figure 50e

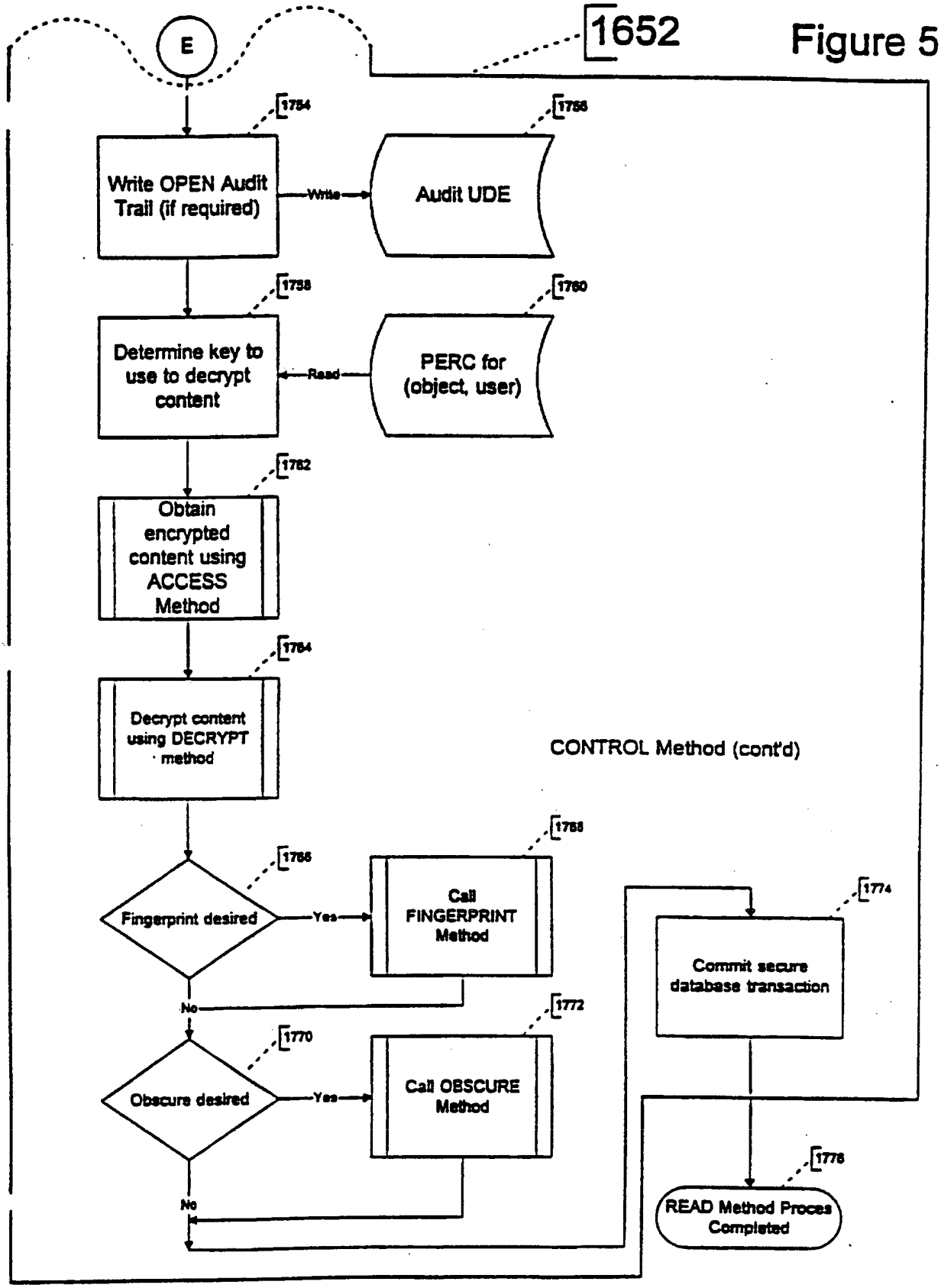

E
1652
1754
Write OPEN Audit Trail (if required)
Write
1756
Audit UDE
1758
Determine key to use to decrypt content
Read
1760
PERC for (object, user)
1762
Obtain encrypted content using ACCESS Method
1764
Decrypt content using DECRYPT method
CONTROL Method (cont'd)
1768
1766
Fingerprint desired
Yes
Call FINGERPRINT Method
No
1772
1770
Obscure desired
Yes
Call OBSCURE Method
No
1774
Commit secure database transaction
1776
READ Method Proces Completed

Figure 50f

WRITE Method Use Process Flow

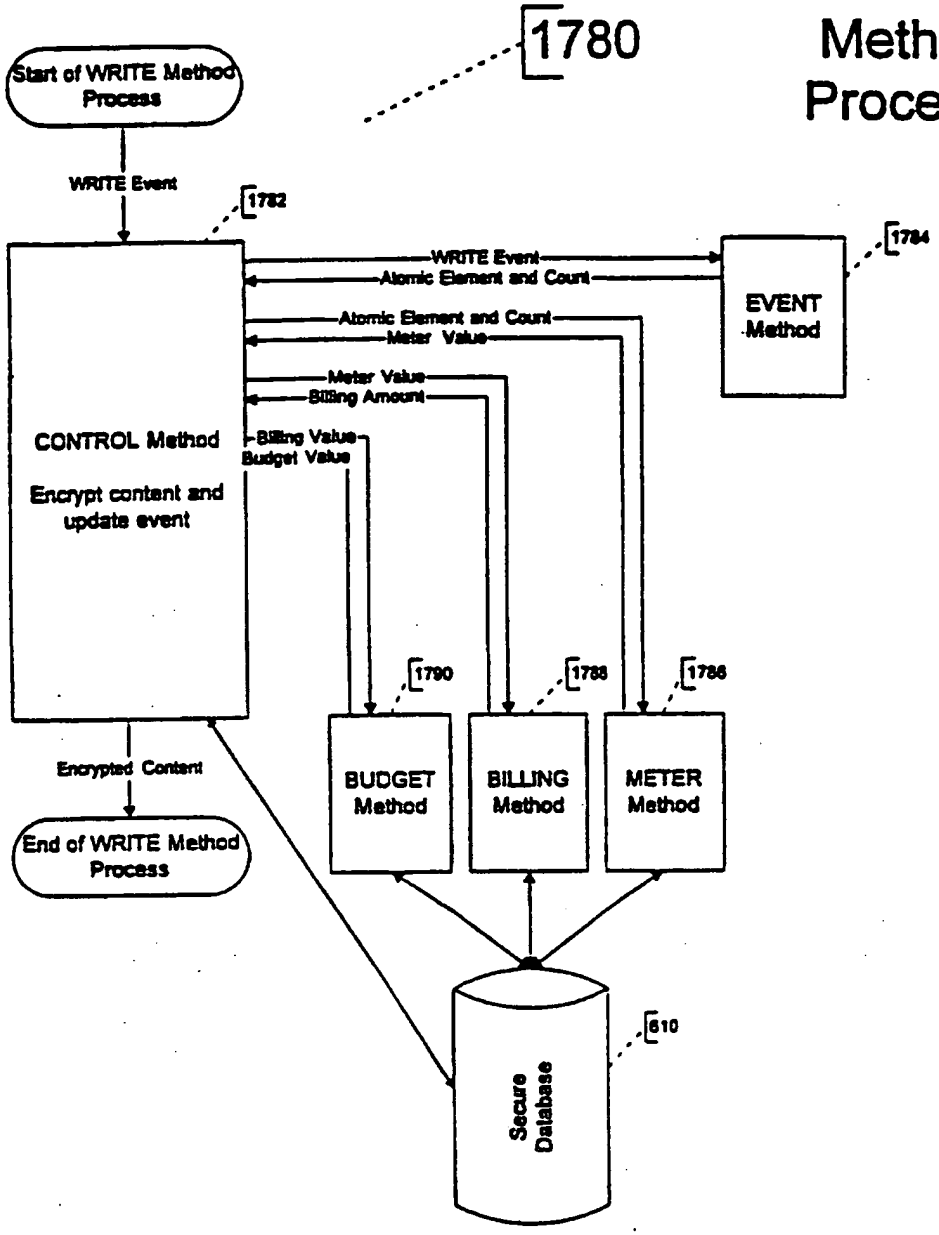


Figure 51

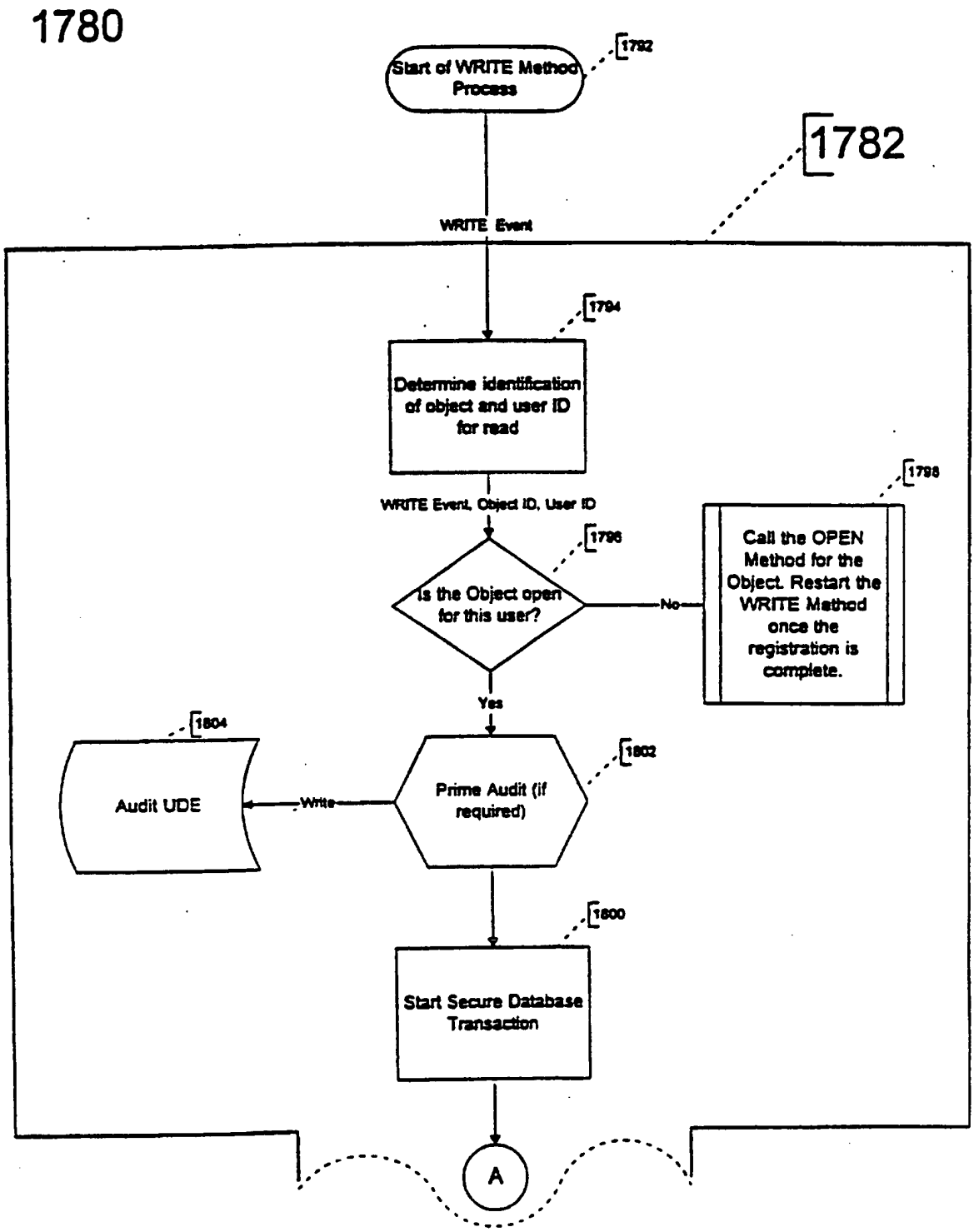

1780
1782
Start of WRITE Method Process
1792
WRITE Event
1794
Determine identification of object and user ID for read
WRITE Event, Object ID, User ID
1796
Is the Object open for this user?
No
1798
Call the OPEN Method for the Object. Restart the WRITE Method once the registration is complete.
Yes
1804
Audit UDE
Write
Prime Audit (if required)
1802
1800
Start Secure Database Transaction
A

Figure 51a

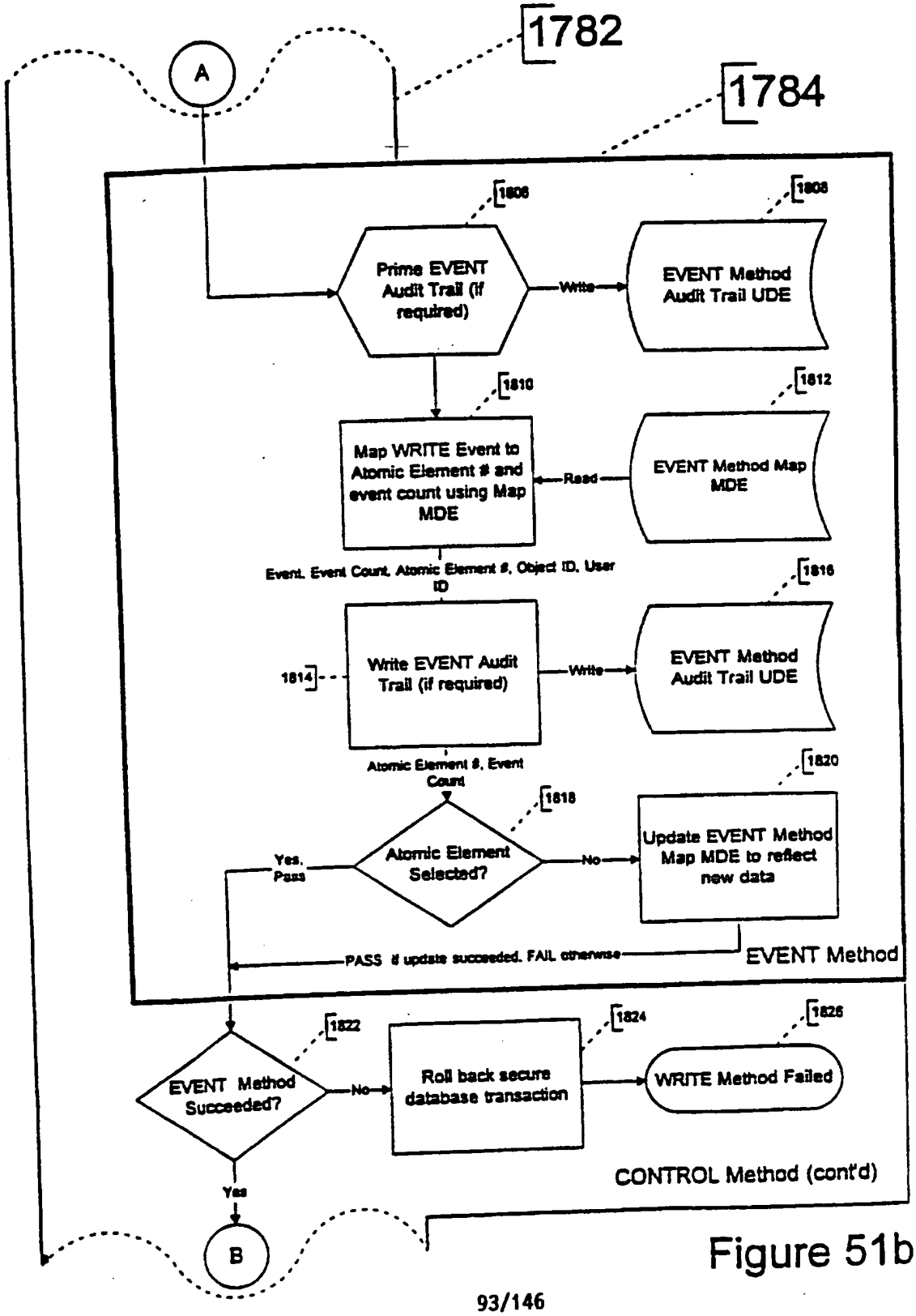

1782
1784
A
1806
Prime EVENT Audit Trail (if required)
Write
1808
EVENT Method Audit Trail UDE
1810
Map WRITE Event to Atomic Element # and event count using Map MDE
Read
1812
EVENT Method Map MDE
Event, Event Count, Atomic Element #, Object ID, User ID
1814
Write EVENT Audit Trail (if required)
Write
1816
EVENT Method Audit Trail UDE
Atomic Element #, Event Count
1818
Atomic Element Selected?
Yes, Pass
No
1820
Update EVENT Method Map MDE to reflect new data
PASS if update succeeded, FAIL otherwise
EVENT Method
1822
EVENT Method Succeeded?
No
1824
Roll back secure database transaction
1826
WRITE Method Failed
Yes
CONTROL Method (cont'd)
B

Figure 51b

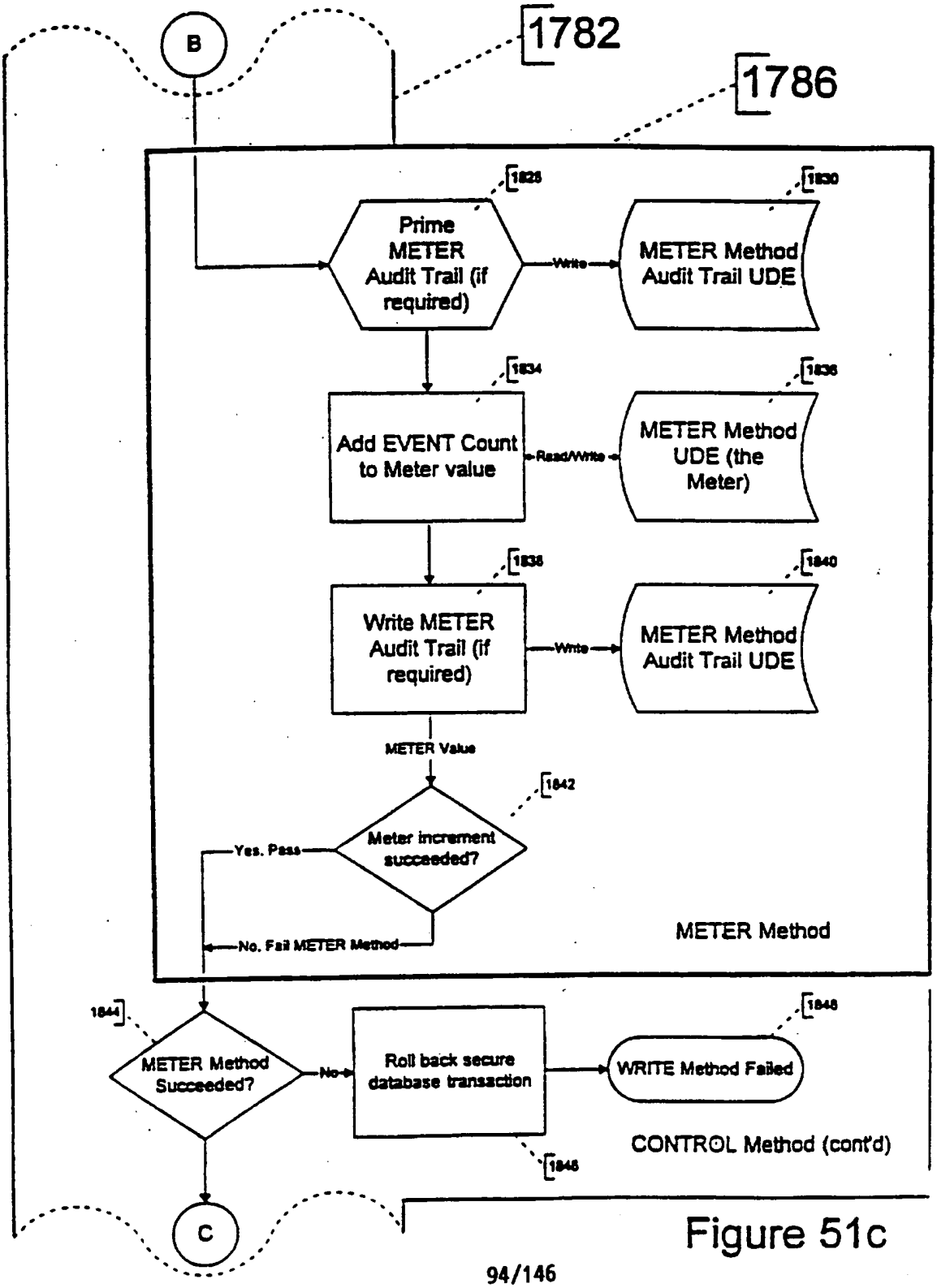

B
1782
1786
1825
Prime METER Audit Trail (if required)
Write
1830
METER Method Audit Trail UDE
1834
Add EVENT Count to Meter value
Read/Write
1836
METER Method UDE (the Meter)
1838
Write METER Audit Trail (if required)
Write
1840
METER Method Audit Trail UDE
METER Value
1842
Meter increment succeeded?
Yes. Pass
No. Fail METER Method
METER Method
1844
METER Method Succeeded?
No
Roll back secure database transaction
1846
WRITE Method Failed
1848
CONTROL Method (cont'd)
C

Figure 51c

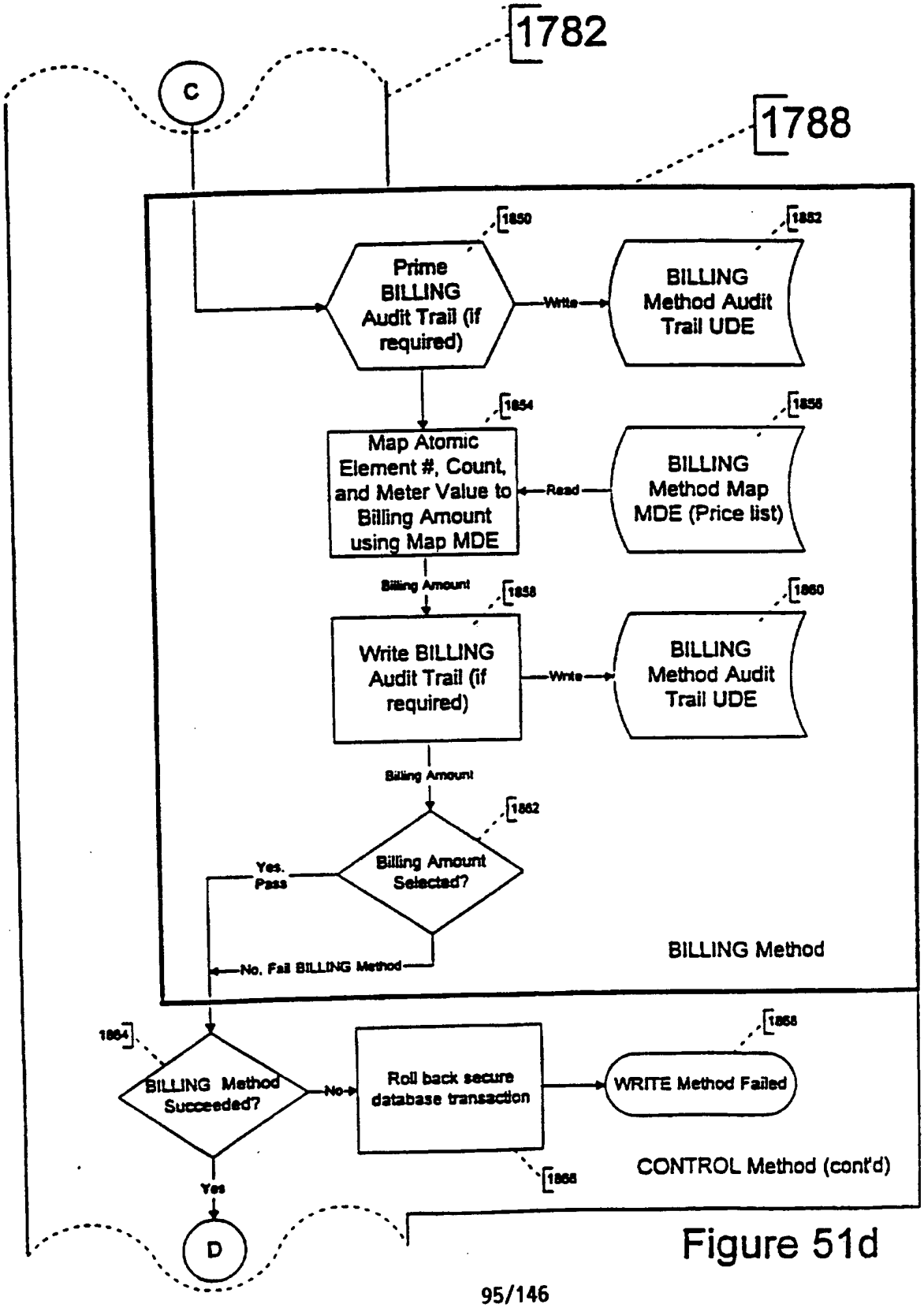

1782
C
1788
1850
Prime BILLING Audit Trail (if required)
Write
1852
BILLING Method Audit Trail UDE
1854
Map Atomic Element #, Count, and Meter Value to Billing Amount using Map MDE
Read
1856
BILLING Method Map MDE (Price list)
Billing Amount
1858
Write BILLING Audit Trail (if required)
Write
1860
BILLING Method Audit Trail UDE
Billing Amount
1862
Billing Amount Selected?
Yes. Pass
No. Fail BILLING Method
BILLING Method
1864
BILLING Method Succeeded?
No
Roll back secure database transaction
1866
WRITE Method Failed
1868
CONTROL Method (cont'd)
Yes
D

Figure 51d

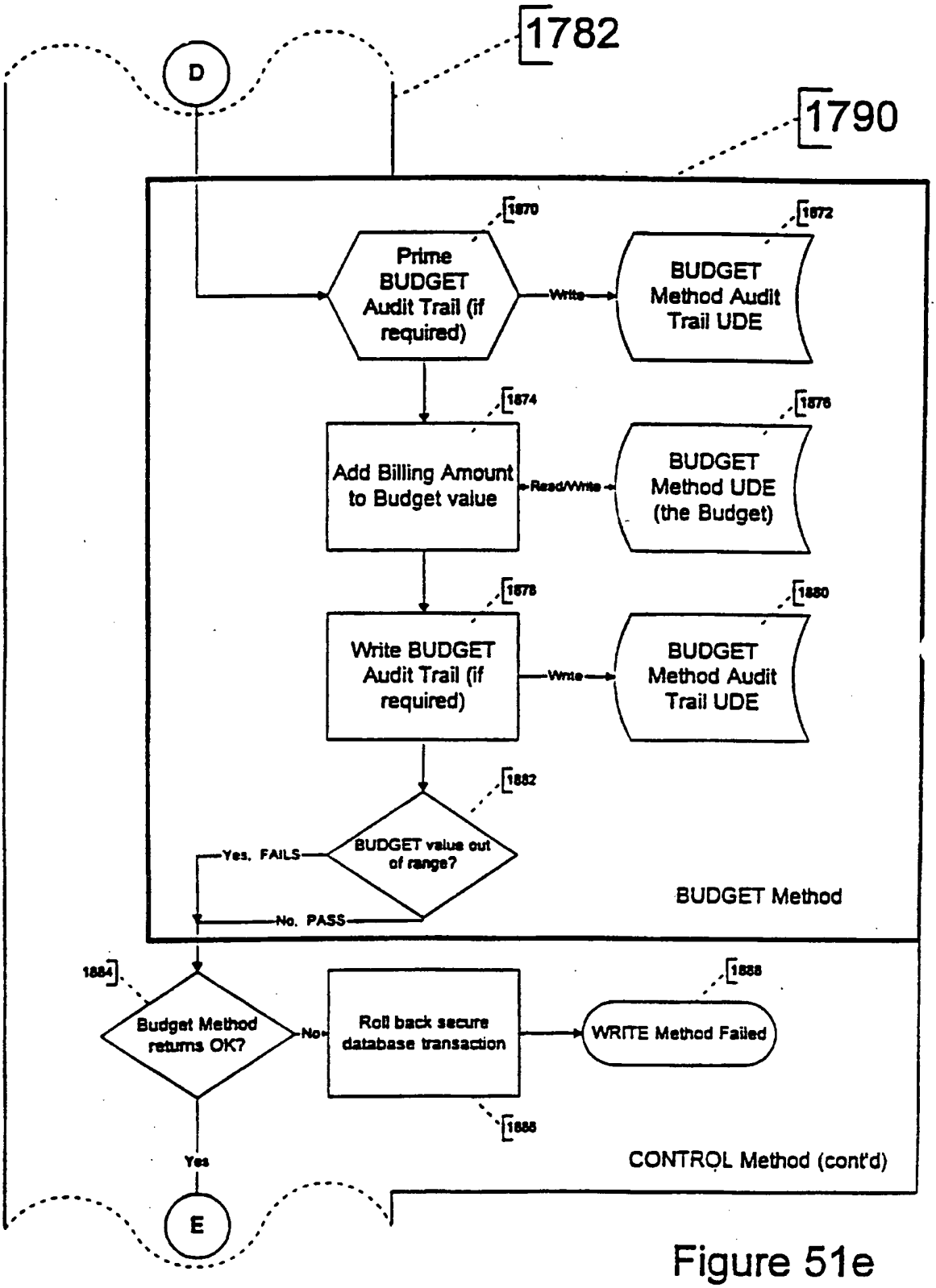

1782
D
1790
1870
Prime BUDGET Audit Trail (if required)
Write
1872
BUDGET Method Audit Trail UDE
1874
Add Billing Amount to Budget value
Read/Write
1876
BUDGET Method UDE (the Budget)
1878
Write BUDGET Audit Trail (if required)
Write
1880
BUDGET Method Audit Trail UDE
1882
BUDGET value out of range?
Yes, FAILS
No, PASS
BUDGET Method
1884
Budget Method returns OK?
No
Roll back secure database transaction
1886
WRITE Method Failed
1888
Yes
CONTROL Method (cont'd)
E

Figure 51e

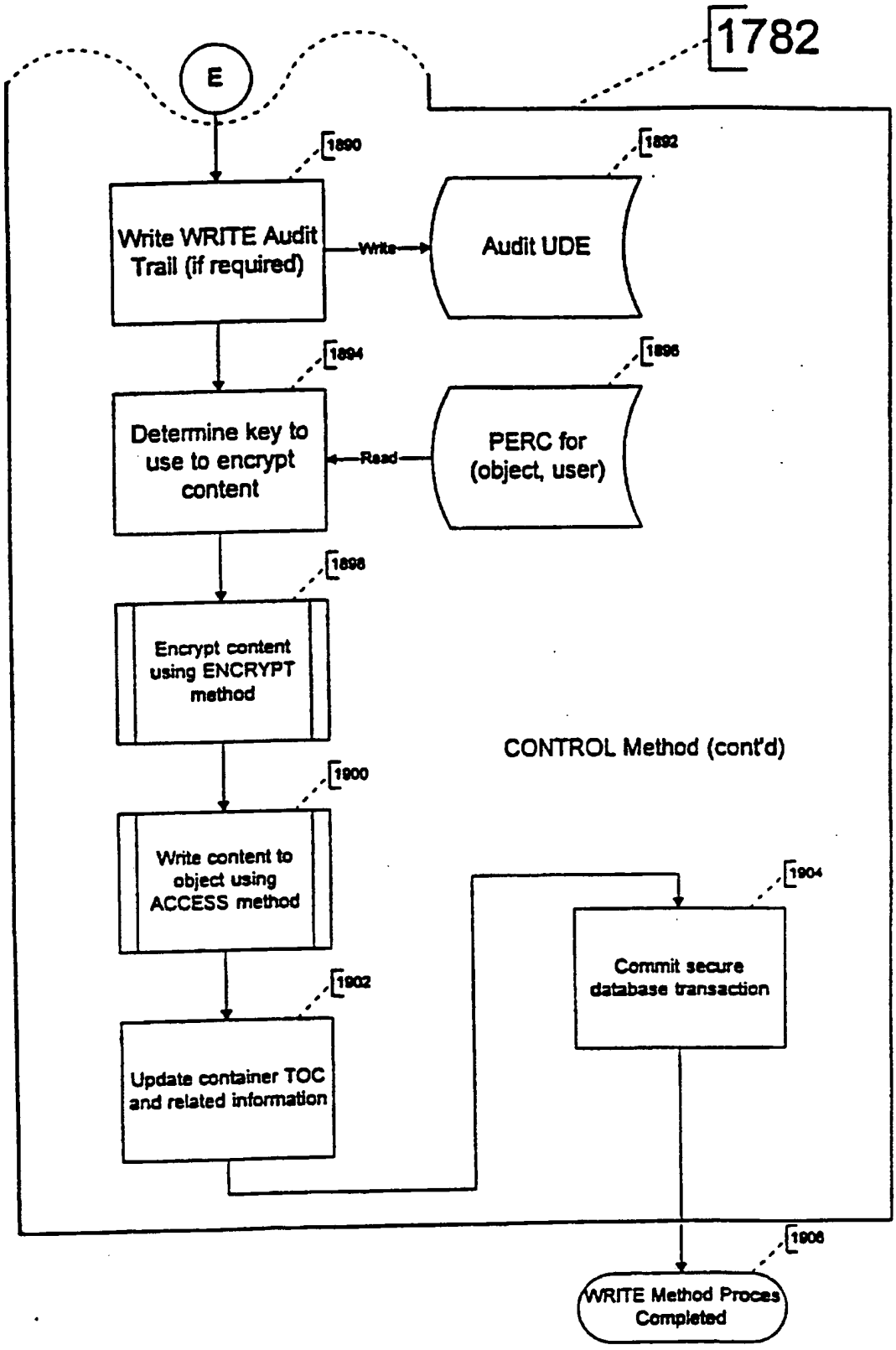
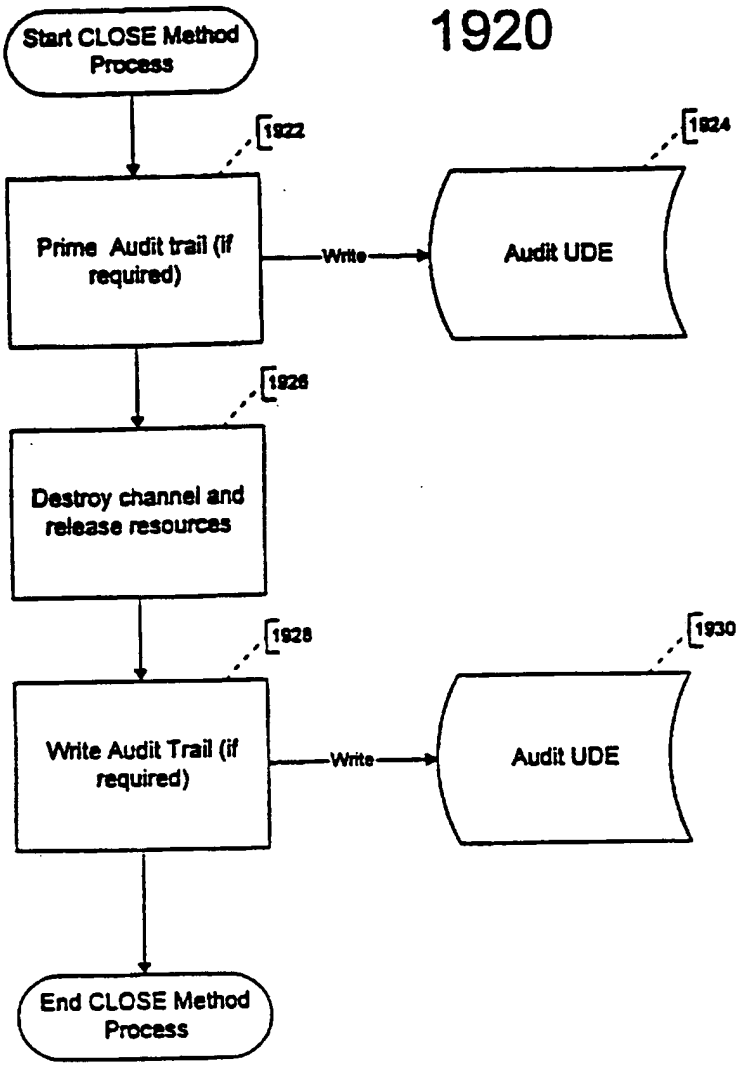
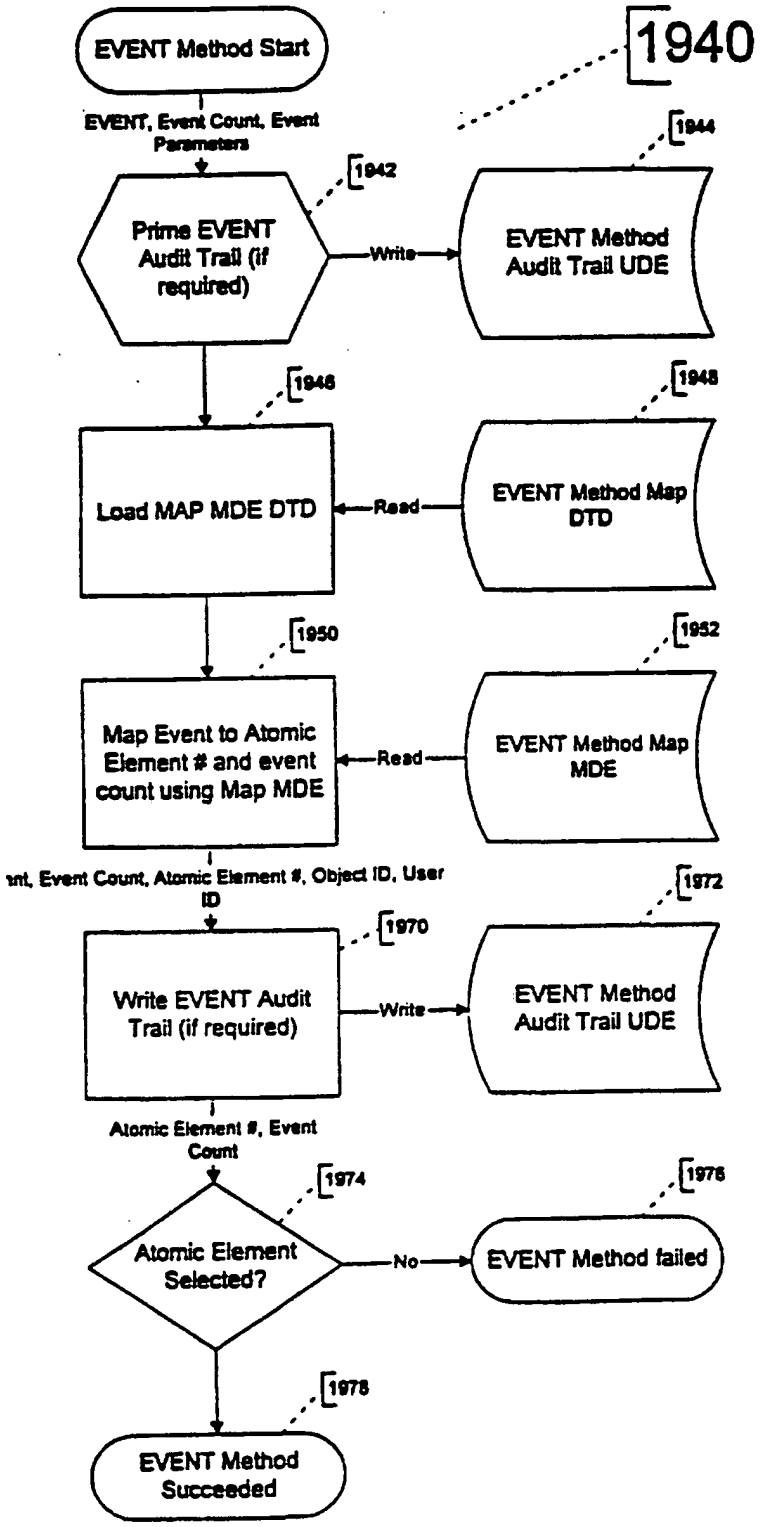

1782
E
1890
Write WRITE Audit Trail (if required)
Write
1892
Audit UDE
1894
Determine key to use to encrypt content
Read
1896
PERC for (object, user)
1898
Encrypt content using ENCRYPT method
CONTROL Method (cont'd)
1900
Write content to object using ACCESS method
1902
Update container TOC and related information
1904
Commit secure database transaction
1906
WRITE Method Proces Completed

Figure 51f



CLOSE Method Process Flow

Figure 52



EVENT Method Process Flows

Figure 53a

Sample EVENT Method Mapping Process

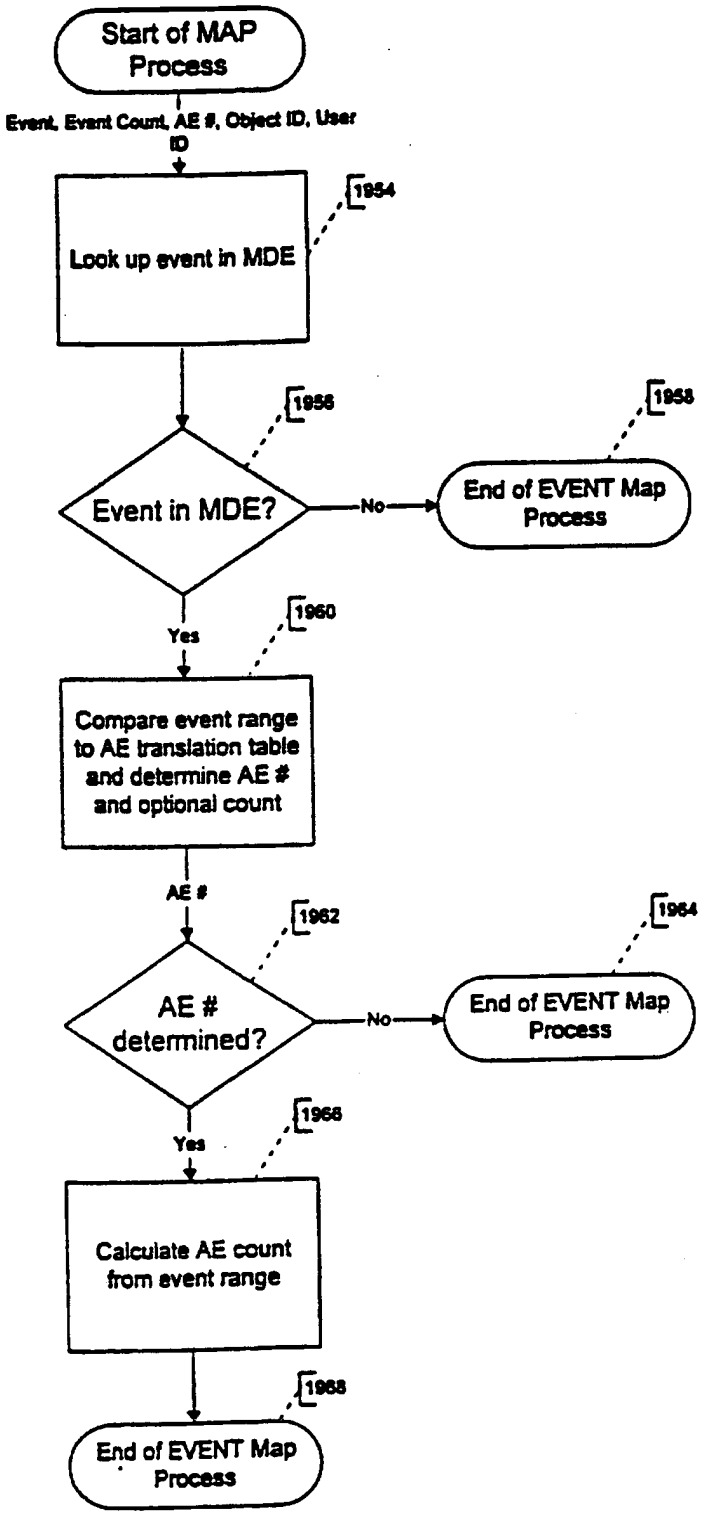


Figure 53b

BILLING Method Process Flows

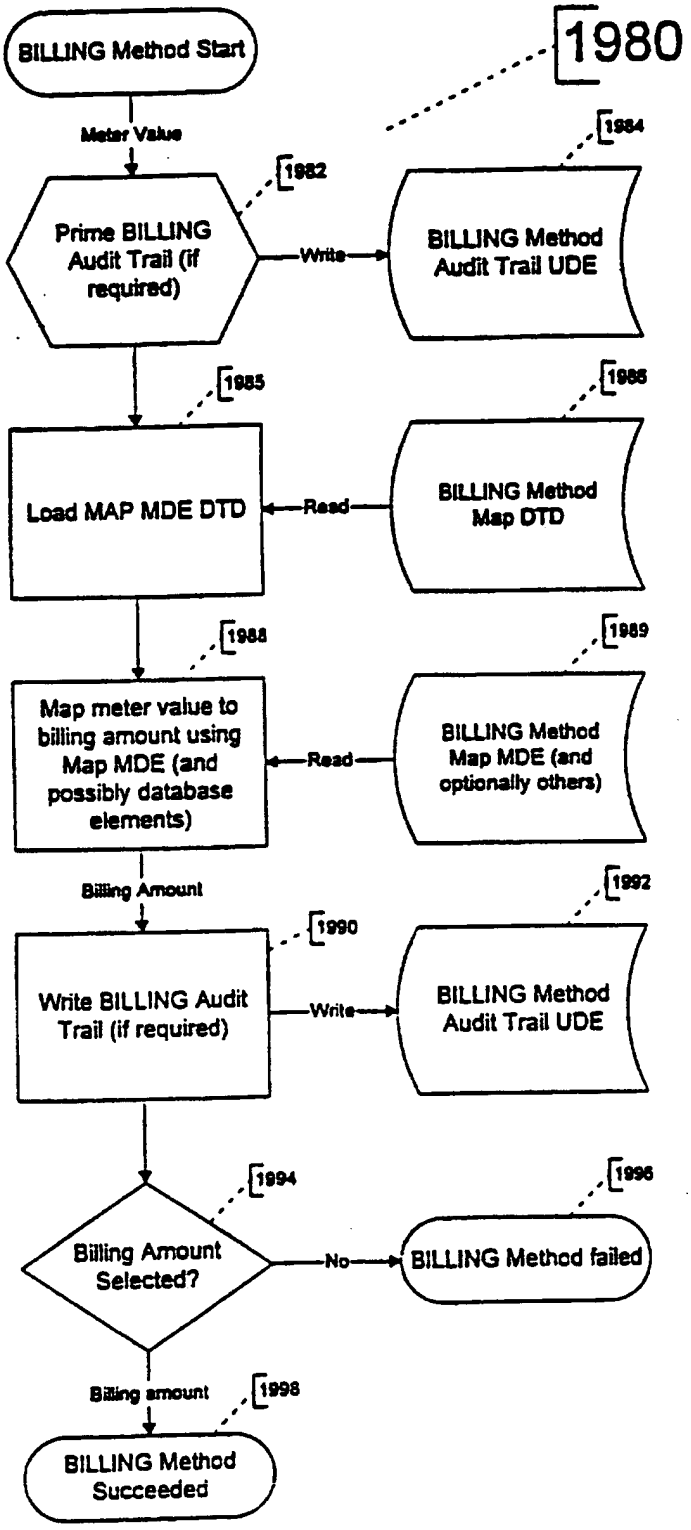
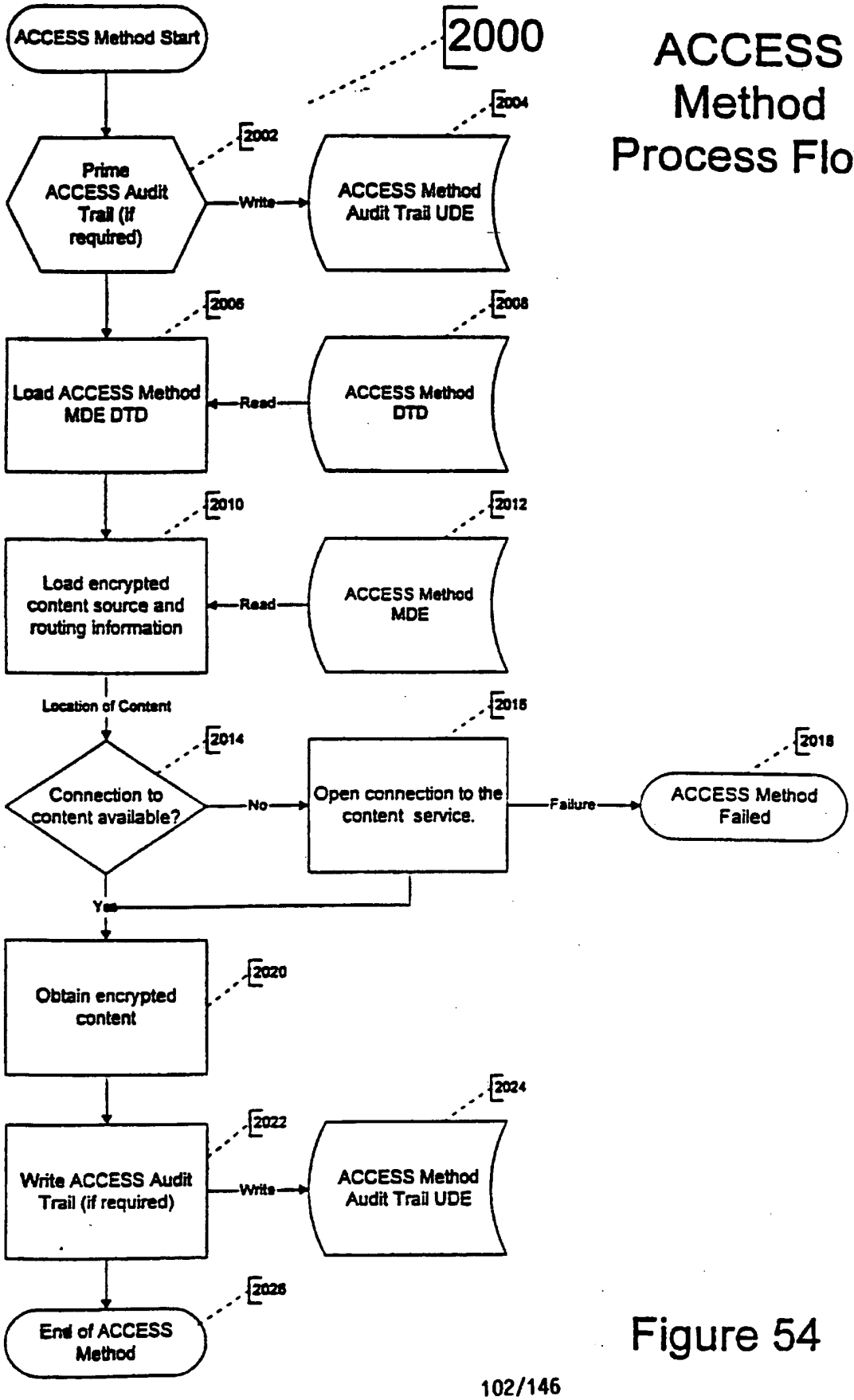


Figure 53c



ACCESS Method Process Flow

Figure 54

DECRYPT Method Process Flow

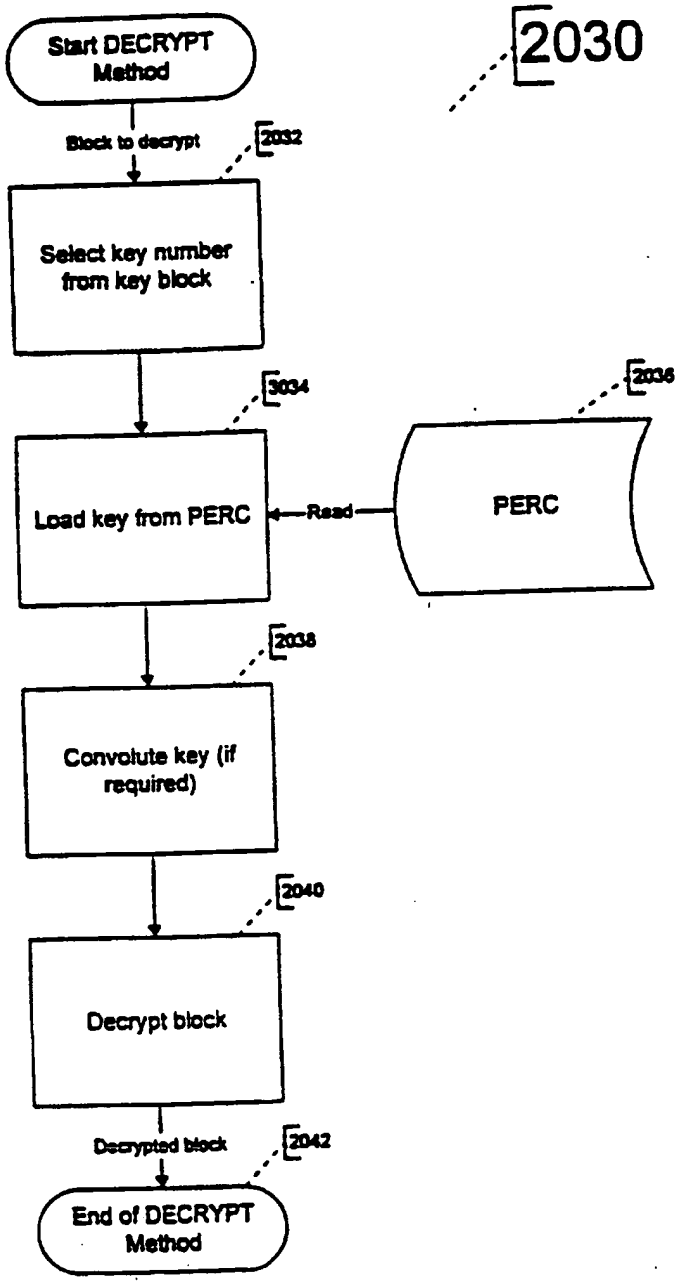


Figure 55a

ENCRYPT Method Process Flow

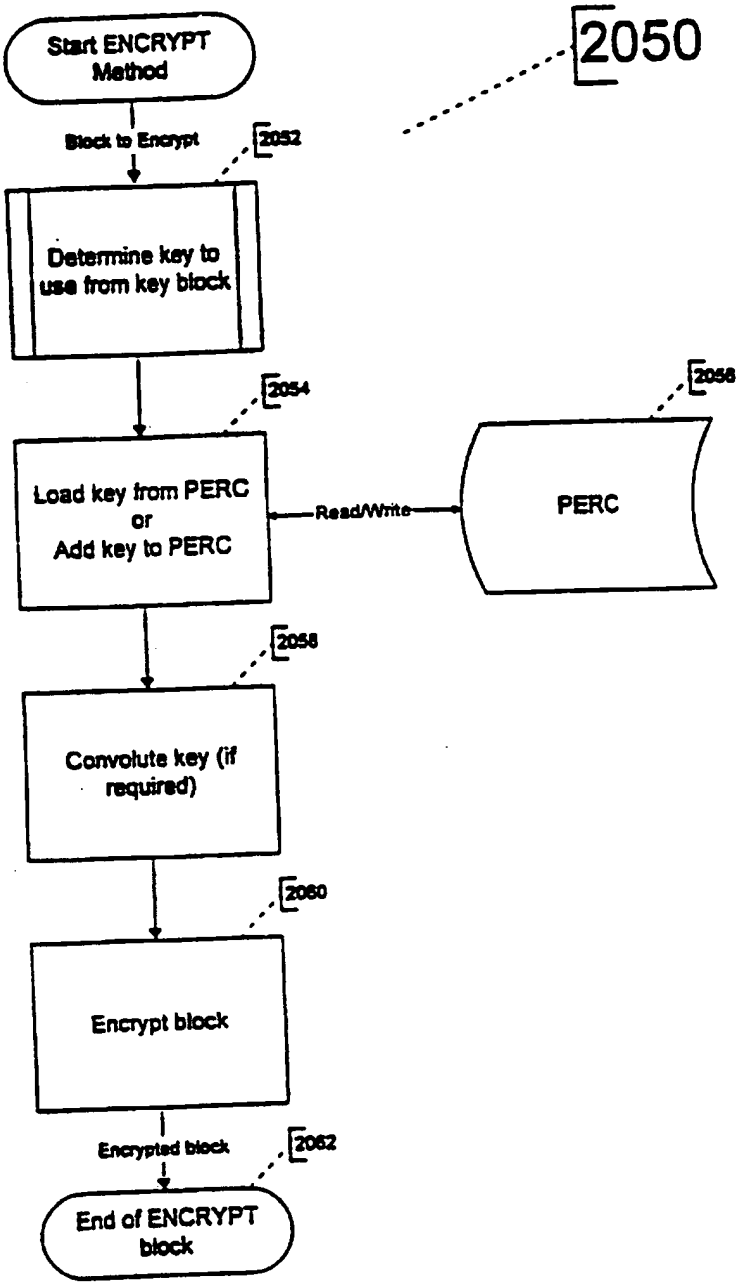
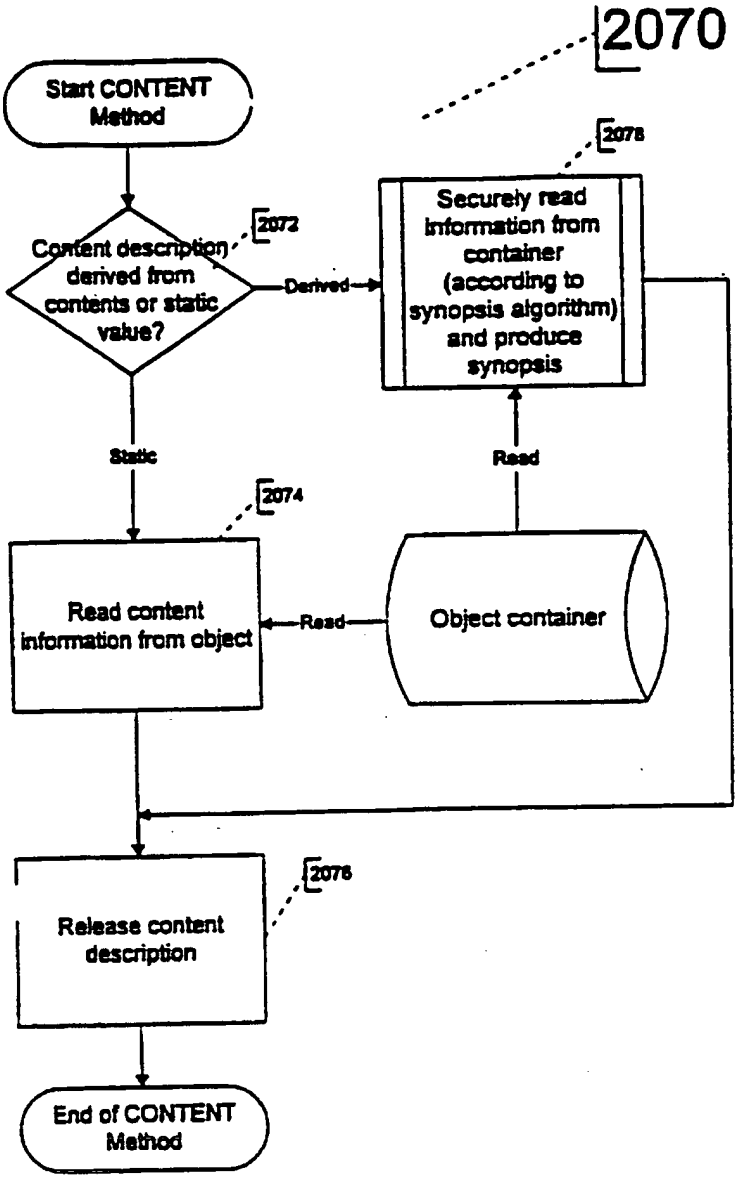


Figure 55b



CONTENT Method Process Flow

Figure 56

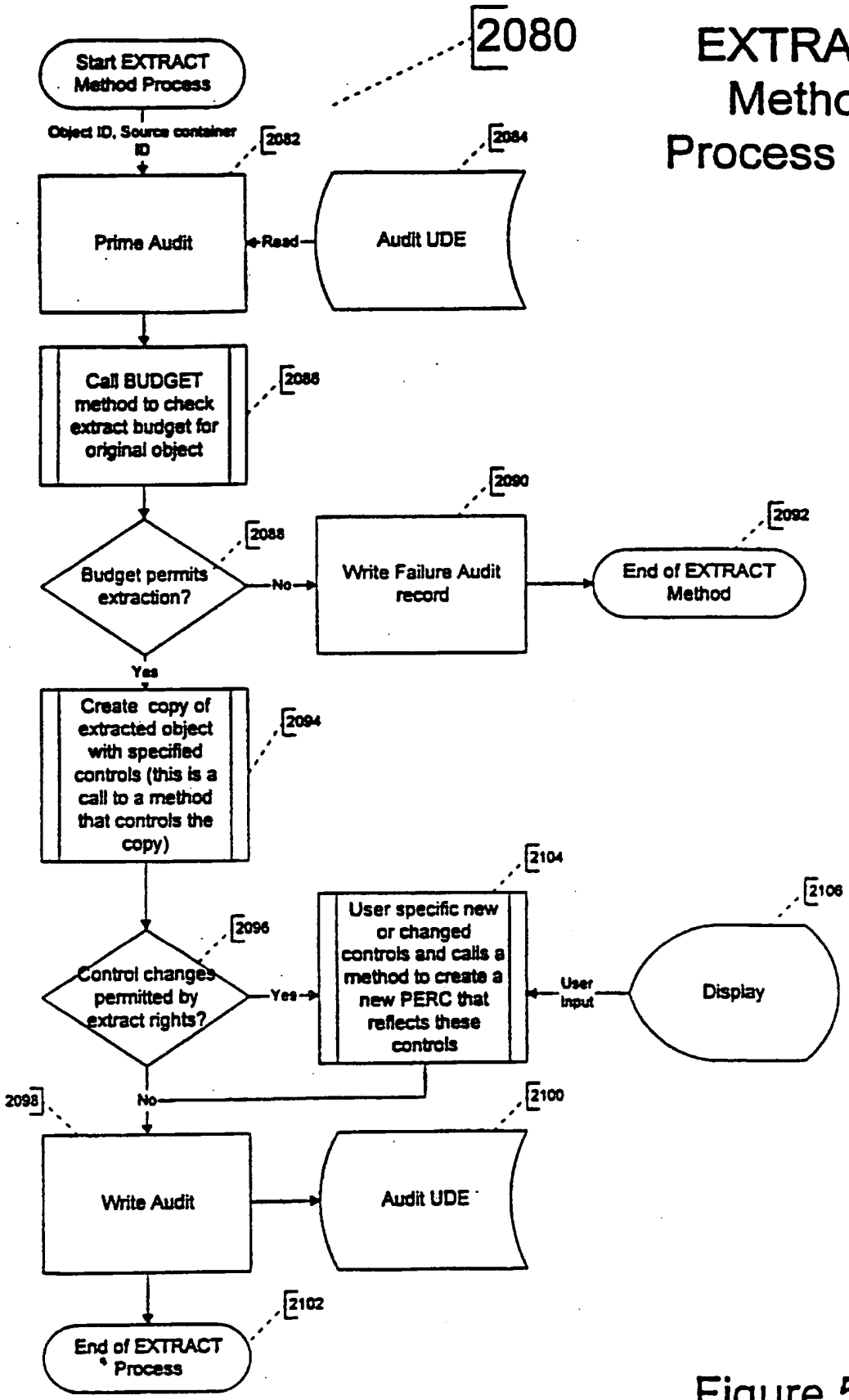

2080
EXTRACT Method Process Flow
Start EXTRACT Method Process
Object ID, Source container ID
2082
2084
Prime Audit
Read
Audit UDE
Call BUDGET method to check extract budget for original object
2086
2090
2088
Budget permits extraction?
No
Write Failure Audit record
2092
End of EXTRACT Method
Yes
Create copy of extracted object with specified controls (this is a call to a method that controls the copy)
2094
2104
2106
2096
Control changes permitted by extract rights?
Yes
User specific new or changed controls and calls a method to create a new PERC that reflects these controls
User Input
Display
2098
No
2100
Write Audit
Audit UDE
2102
End of EXTRACT Process

Figure 57a

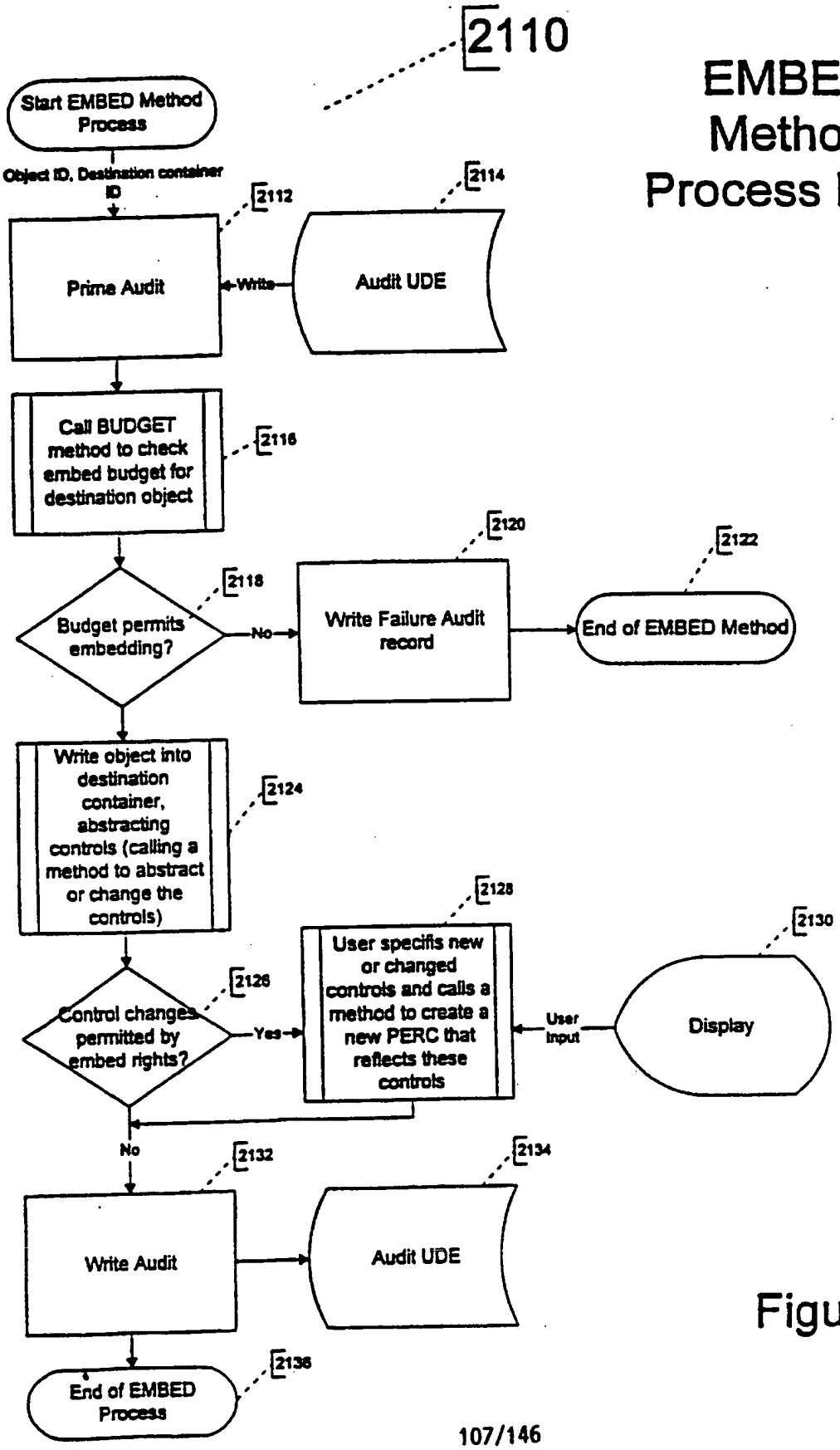
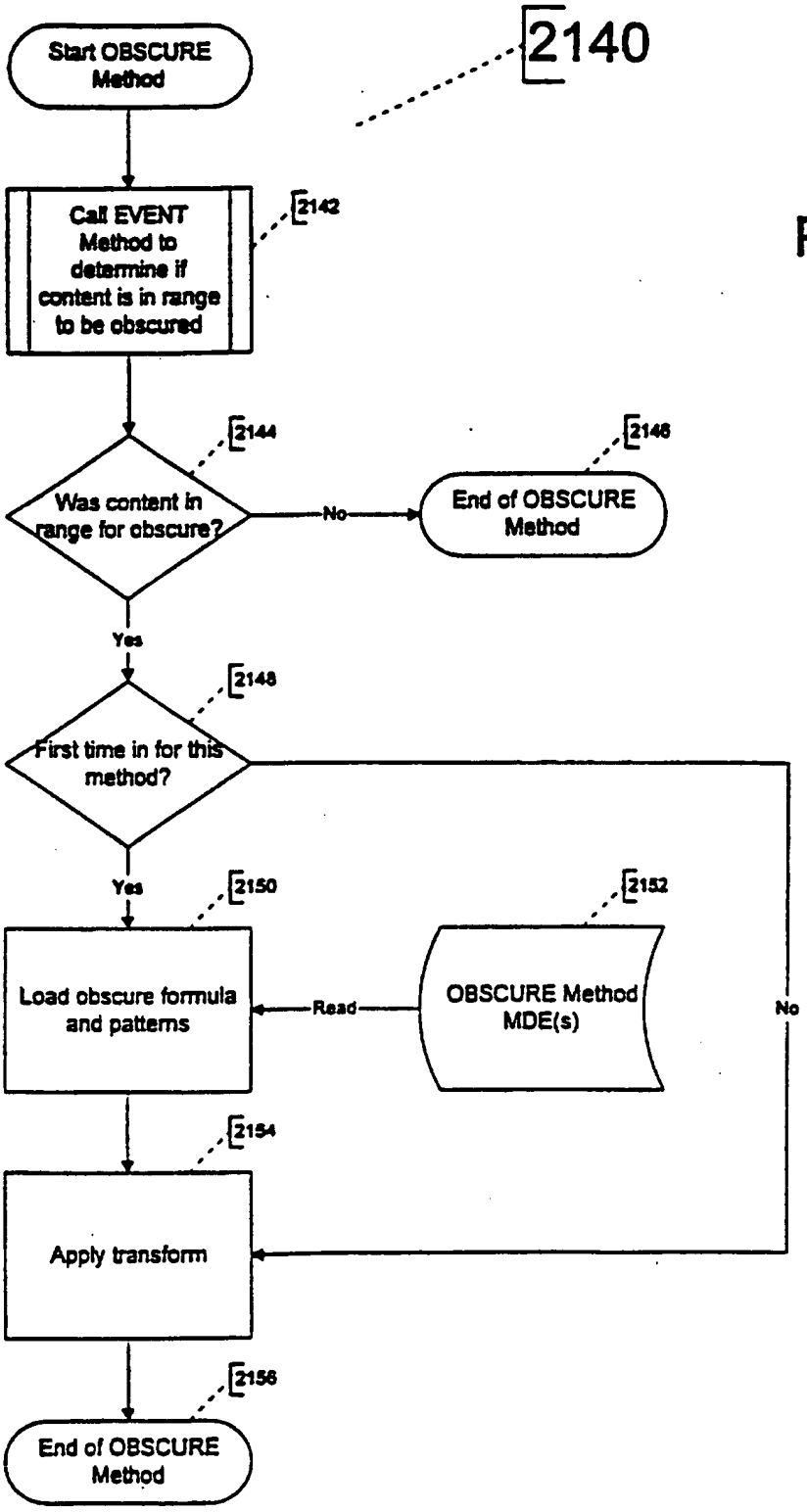
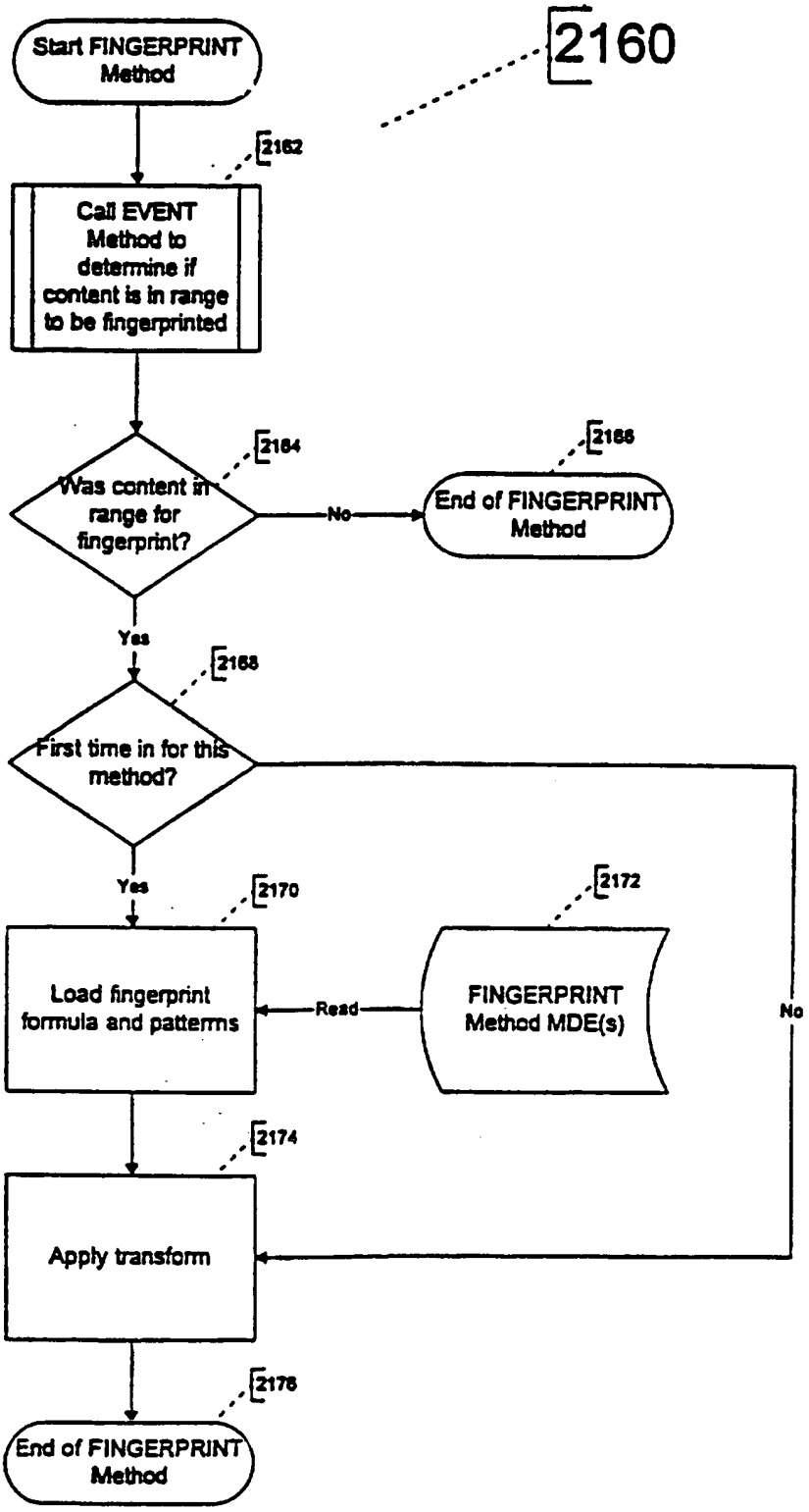

2110
EMBED Method Process Flow
Start EMBED Method Process
Object ID, Destination container ID
2112
Prime Audit
Write
2114
Audit UDE
Call BUDGET method to check embed budget for destination object
2116
2118
Budget permits embedding?
No
2120
Write Failure Audit record
2122
End of EMBED Method
Write object into destination container, abstracting controls (calling a method to abstract or change the controls)
2124
2126
Control changes permitted by embed rights?
Yes
2128
User specifis new or changed controls and calls a method to create a new PERC that reflects these controls
User Input
2130
Display
No
2132
Write Audit
2134
Audit UDE
2136
End of EMBED Process

Figure 57b



OBSCURE Method Process Flow

Figure 58a



FINGERPRINT Method Process Flow

Figure 58b

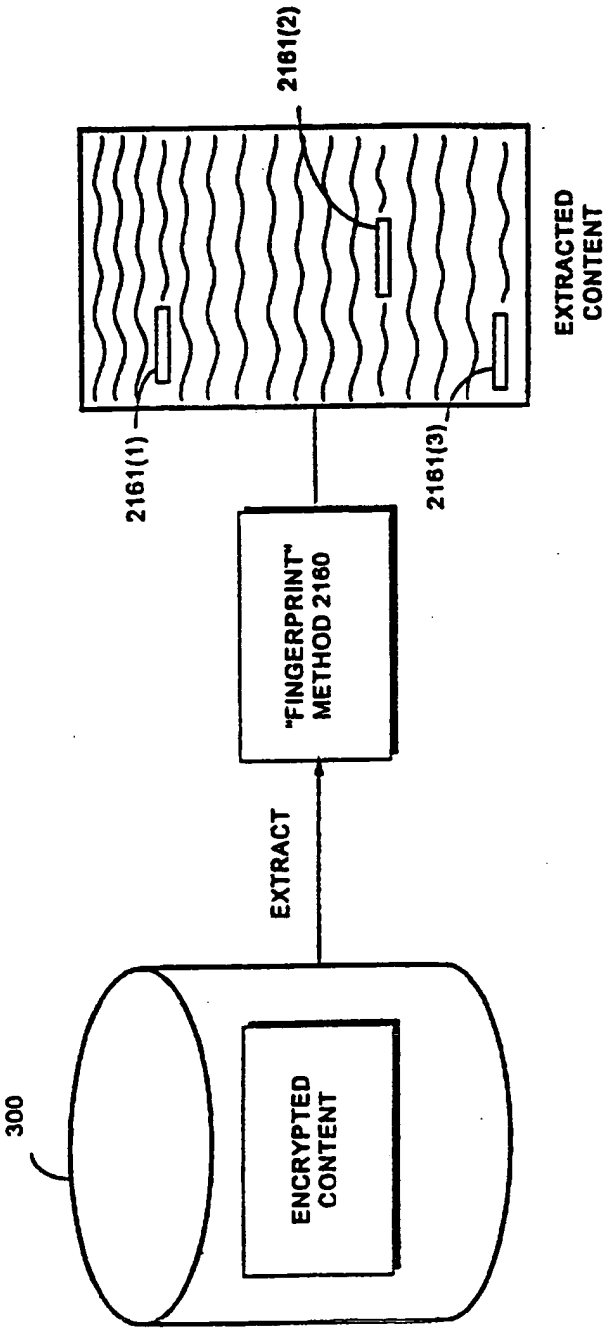
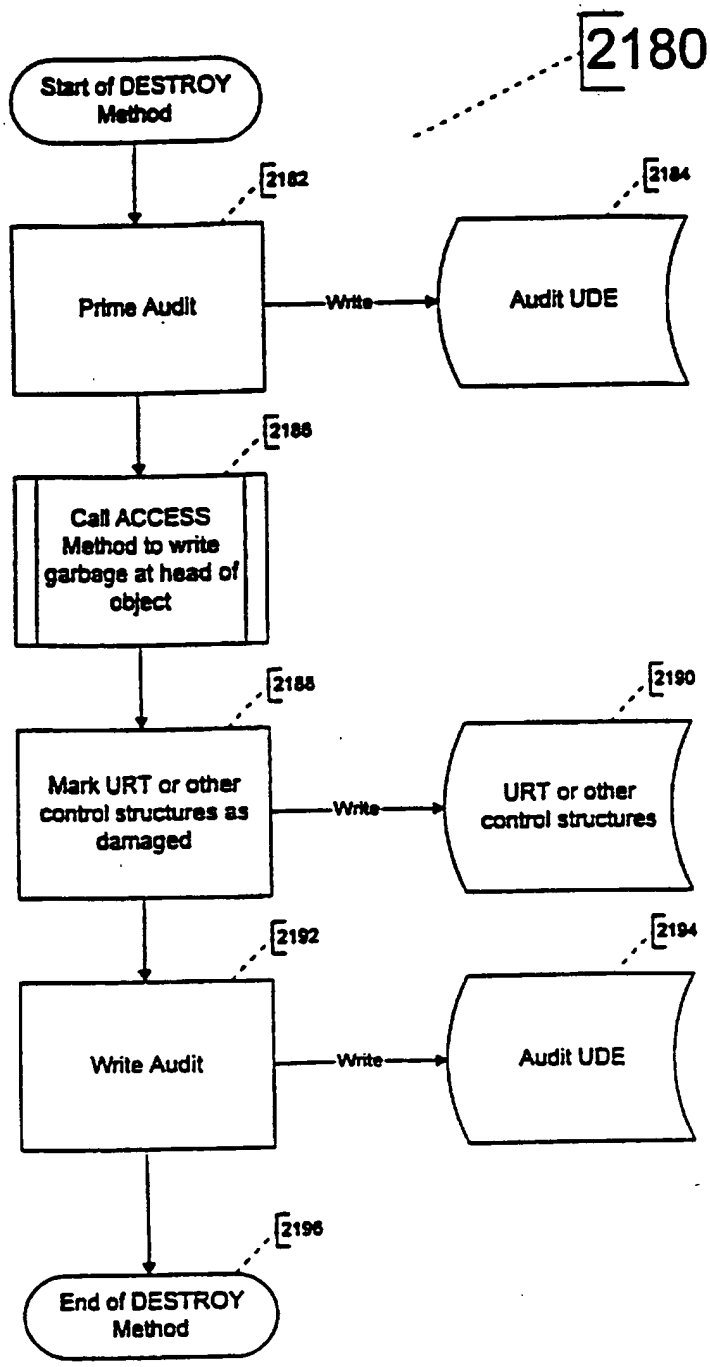
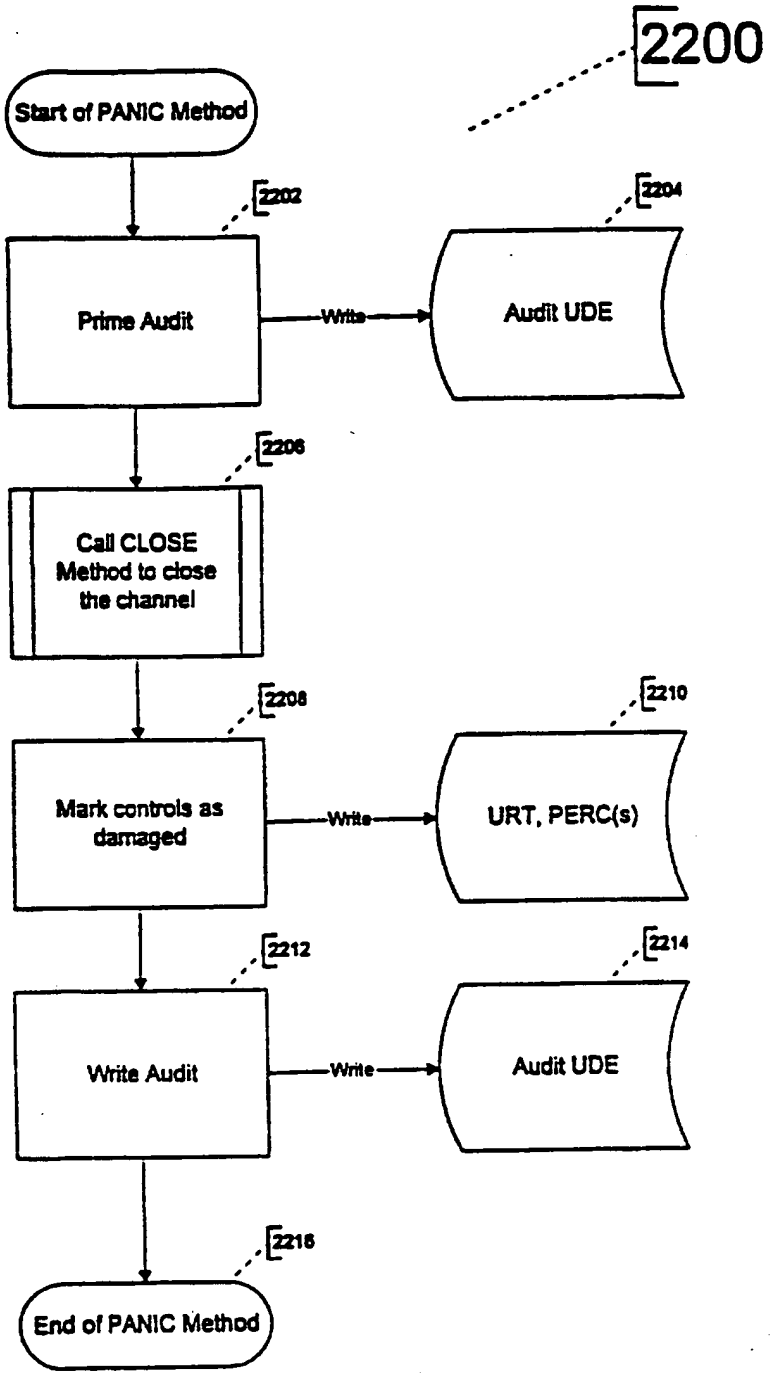

2161(2)
EXTRACTED CONTENT
2161(1)
2161(3)
"FINGERPRINT" METHOD 2160
EXTRACT
300
ENCRYPTED CONTENT

FIG. 58C



DESTROY Method Process Flow

Figure 59



PANIC Method Process Flow

Figure 60

METER Method Use Process Flow

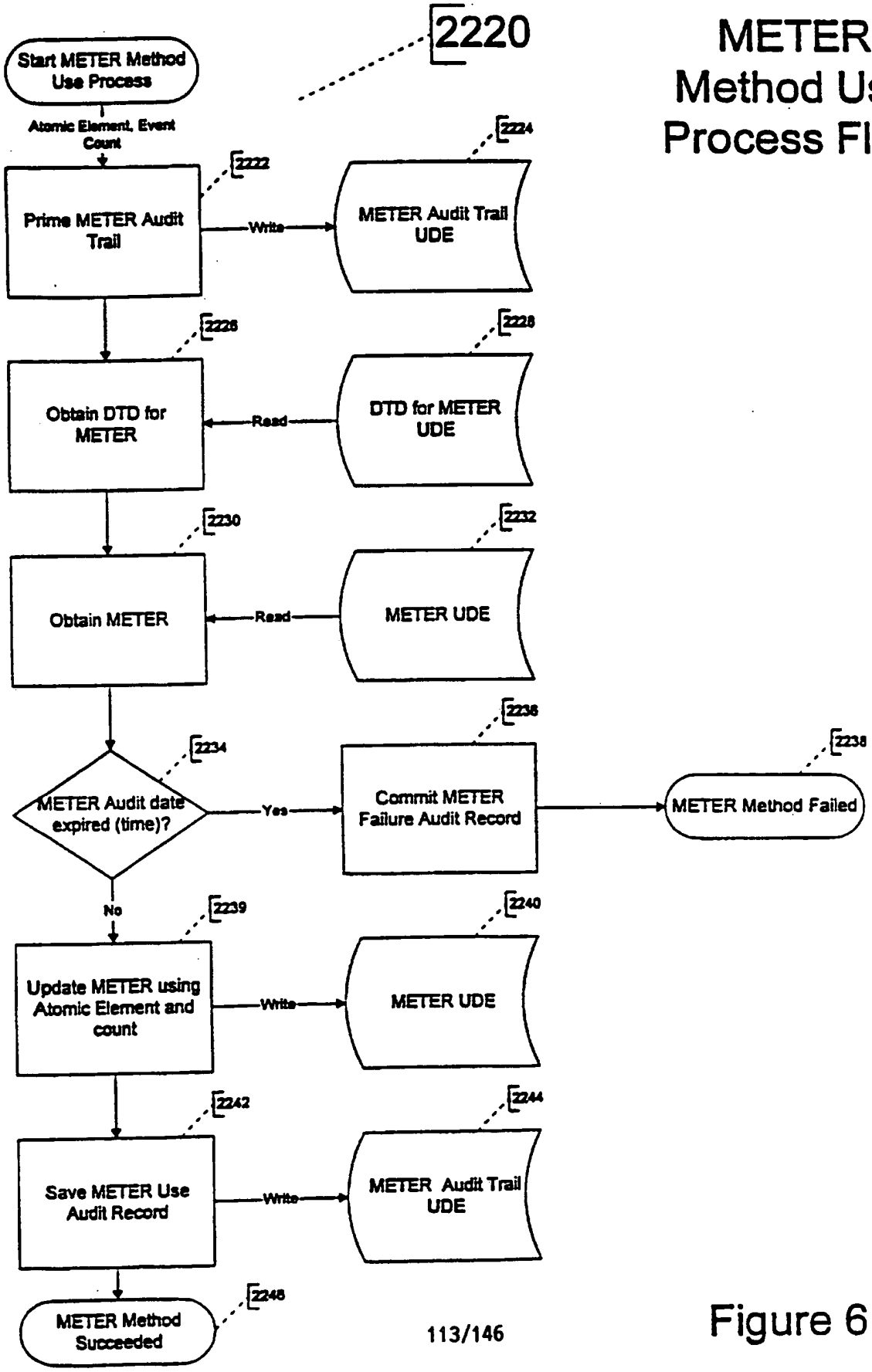
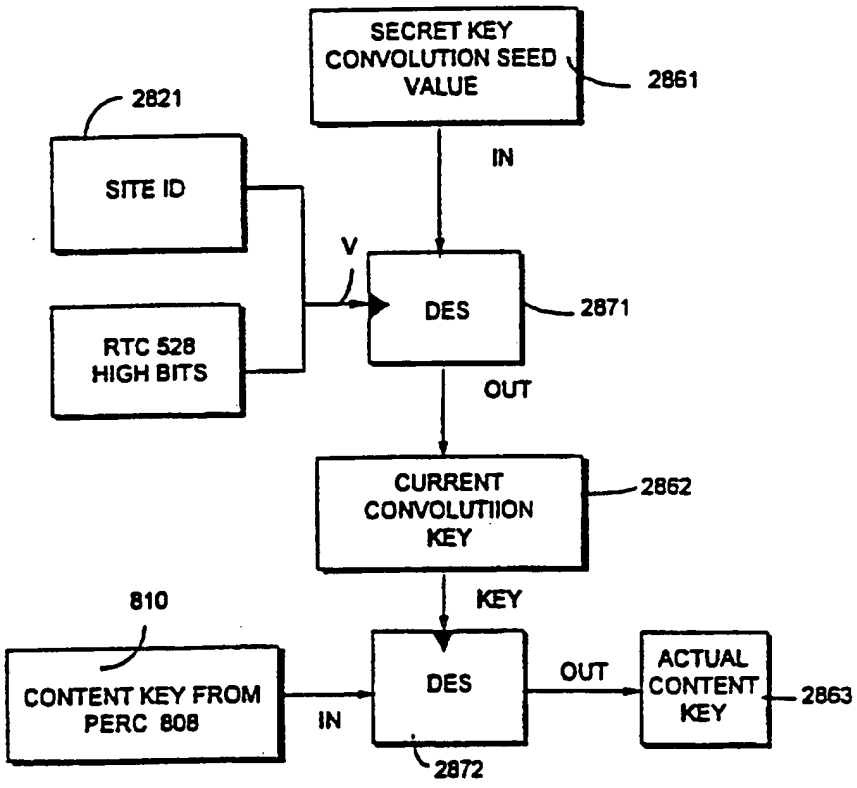


Figure 61

FIG. 62

KEY CONVOLUTION PROCESS



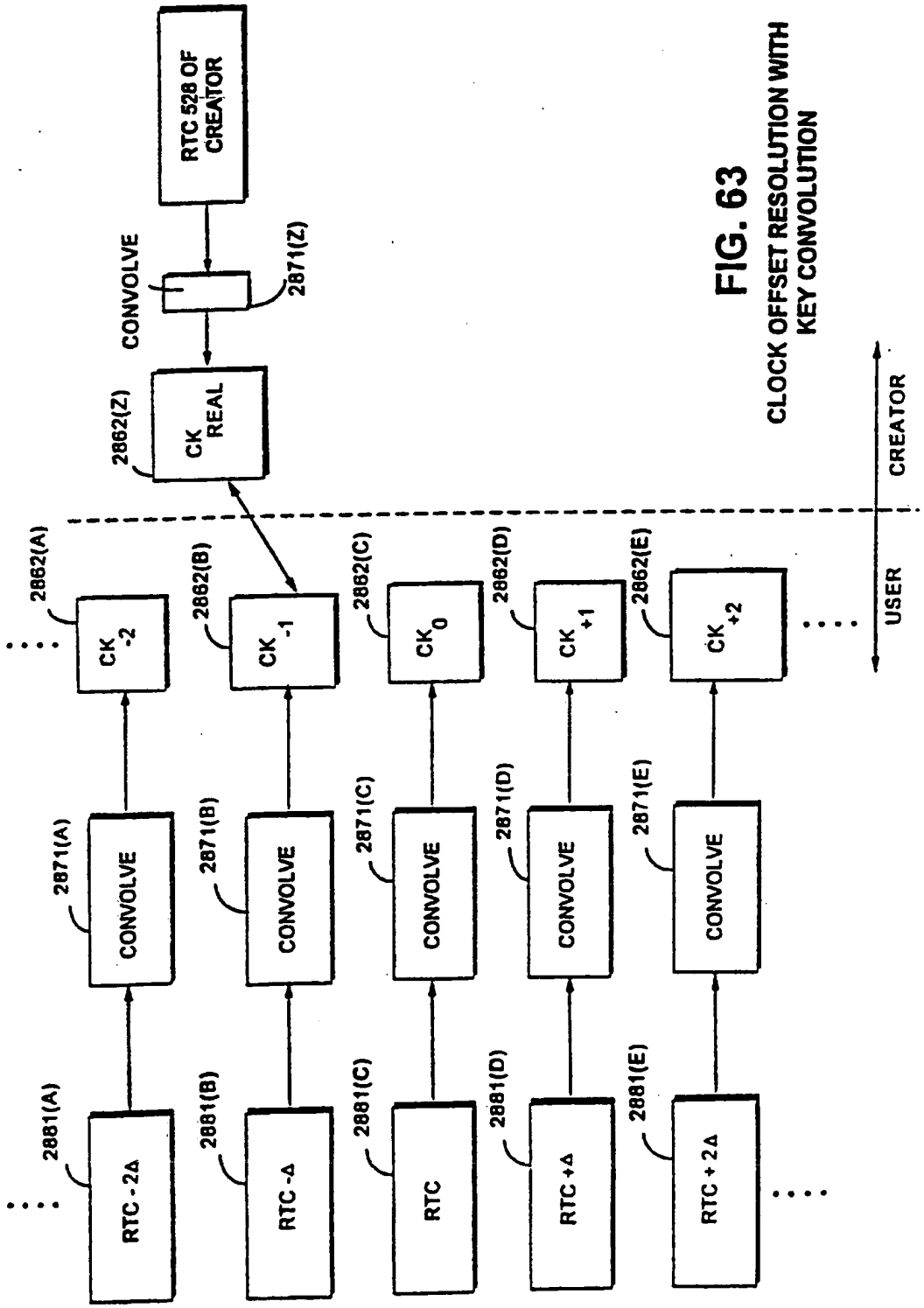


FIG. 63
CLOCK OFFSET RESOLUTION WITH KEY CONVOLUTION

FIG. 64 SPU KEY INITIALIZATION/INSTALLATION

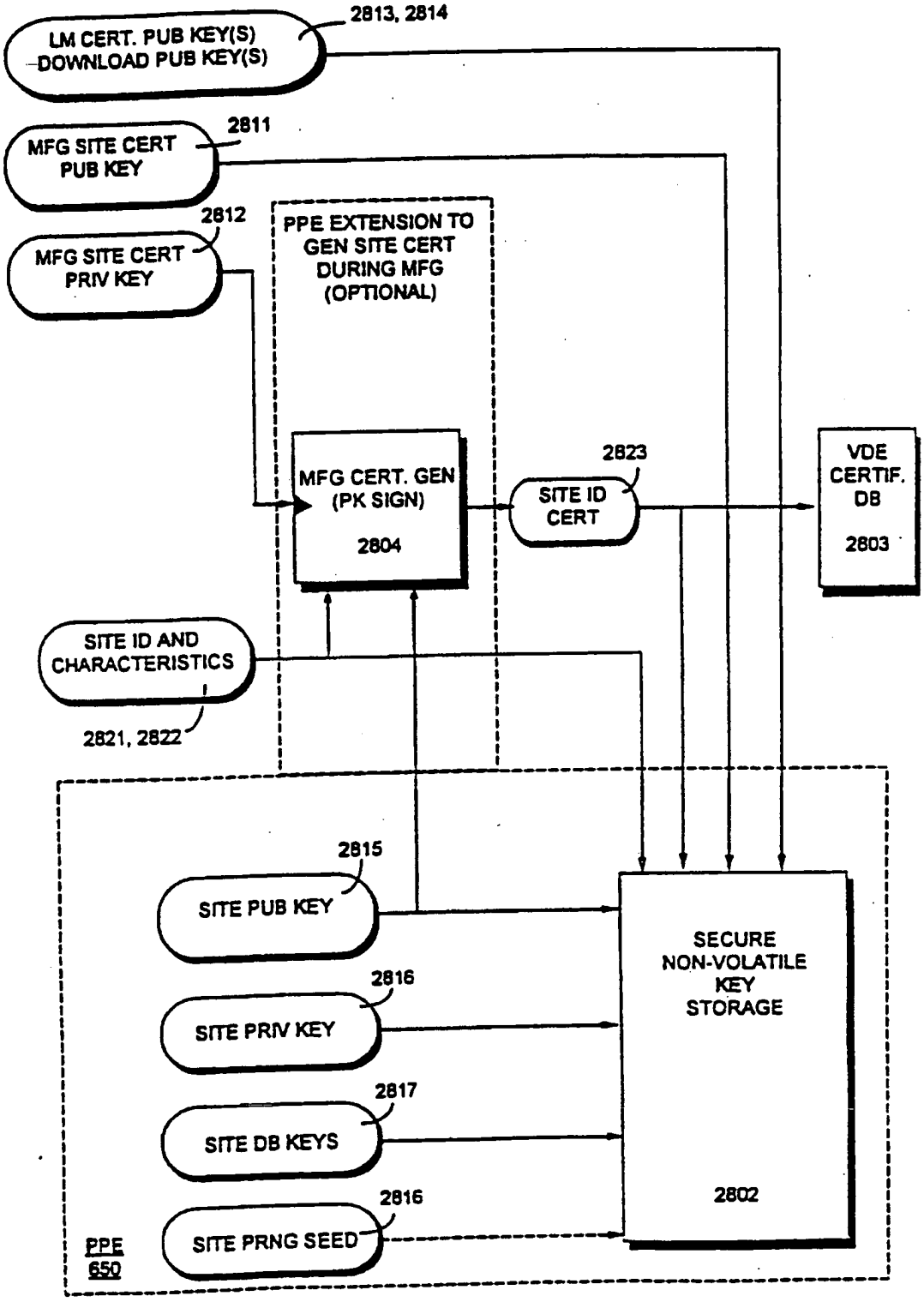
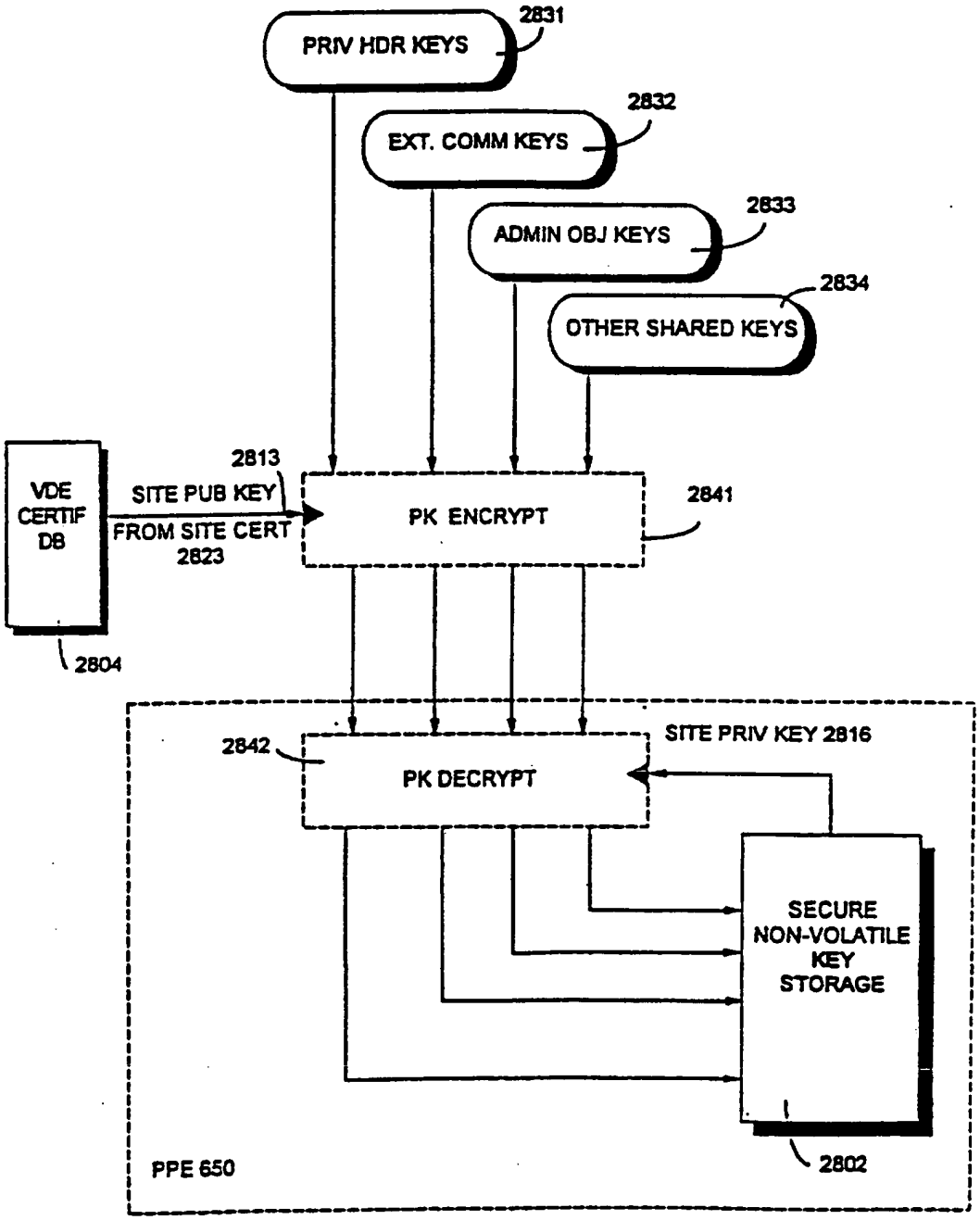


FIG. 65 KEY INSTALLATION & UPDATE



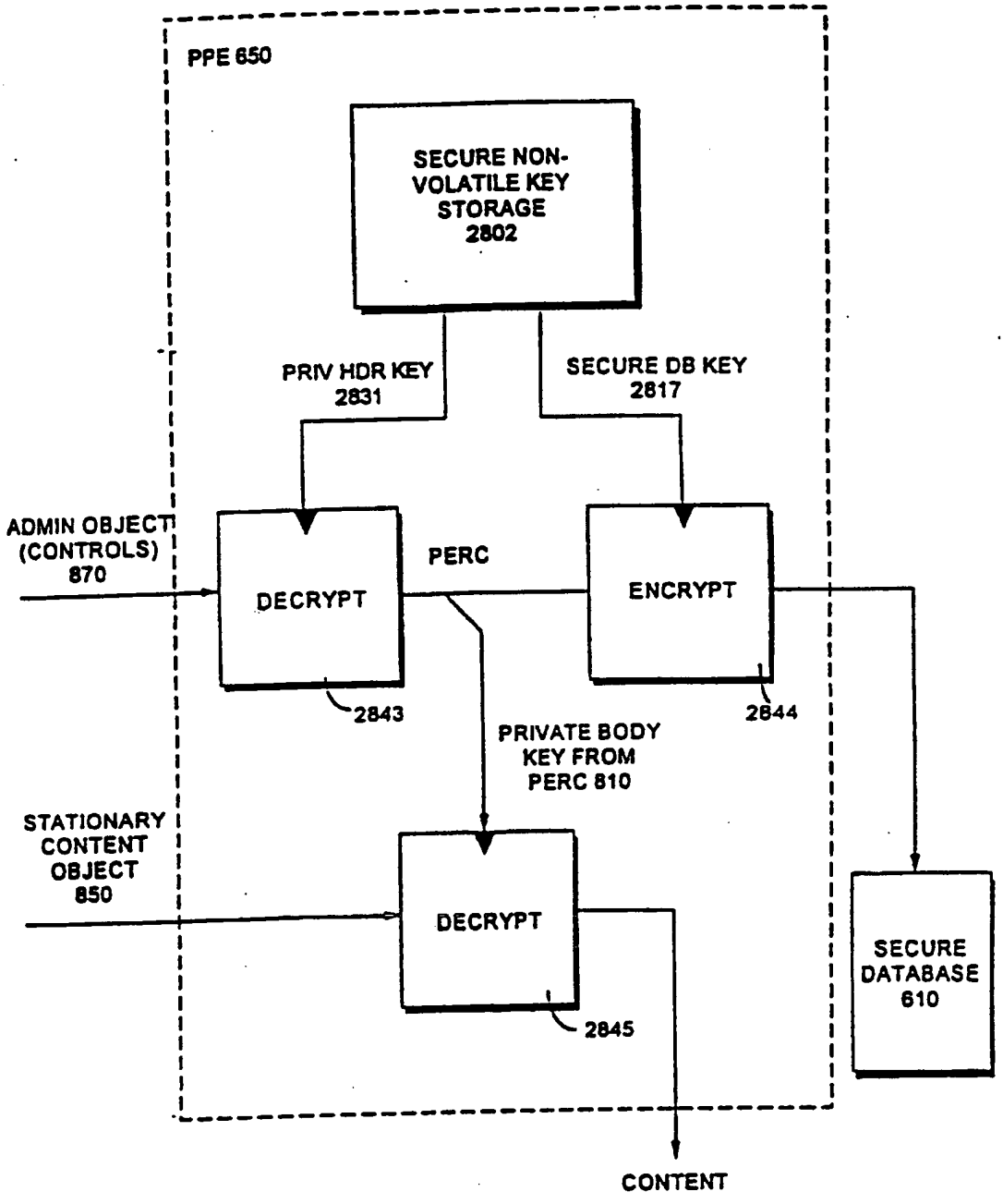


FIG. 66 STATIONARY OBJECT DECRYPTION

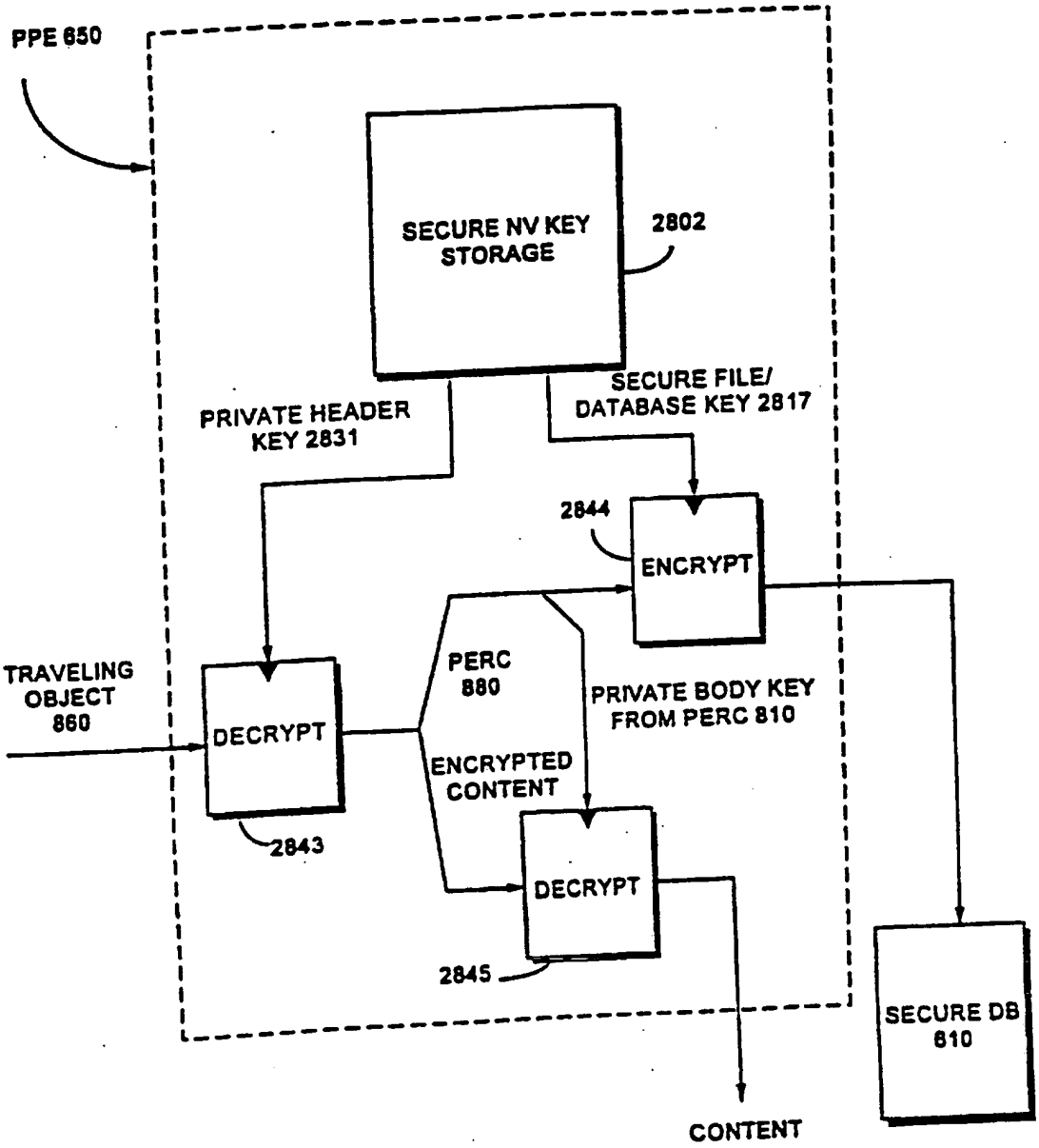
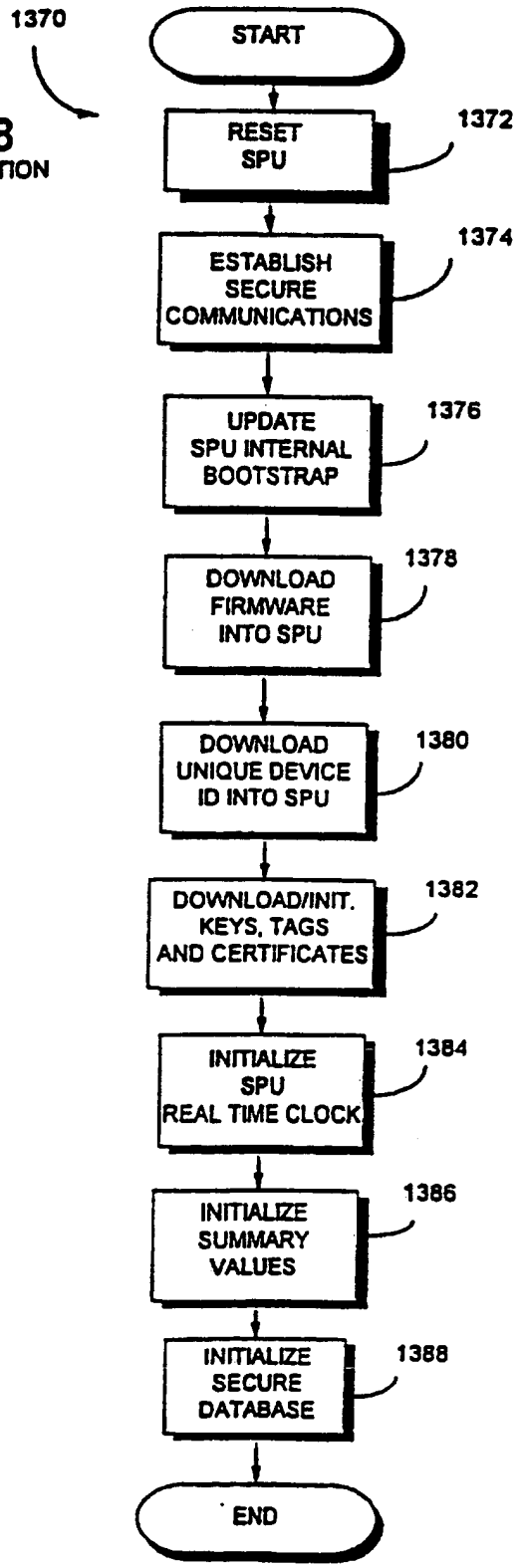


FIG. 67 TRAVELING OBJECT DECRYPTION

FIG. 68
SPU INITIALIZATION



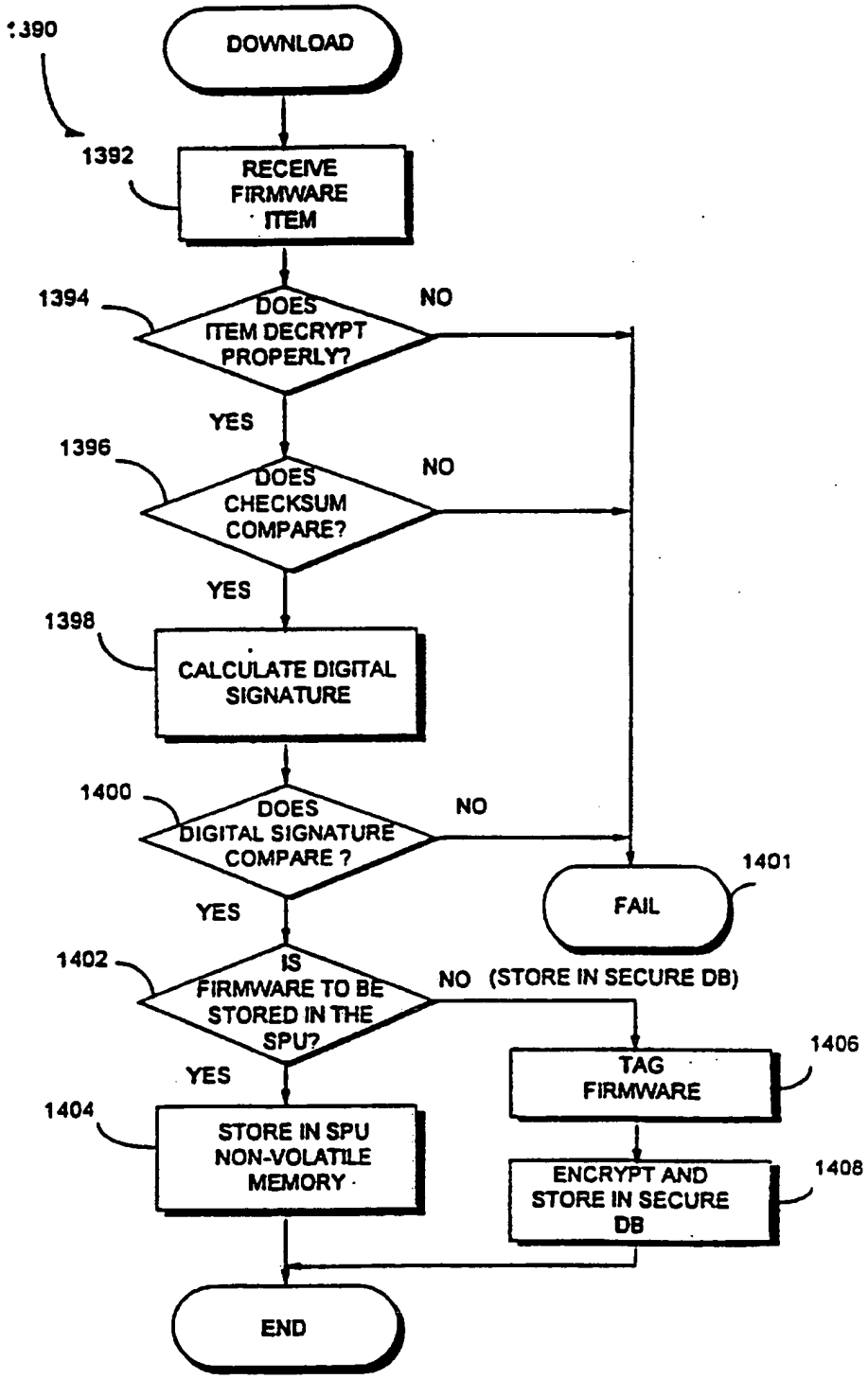


FIG. 69
SPU FIRMWARE DOWNLOAD

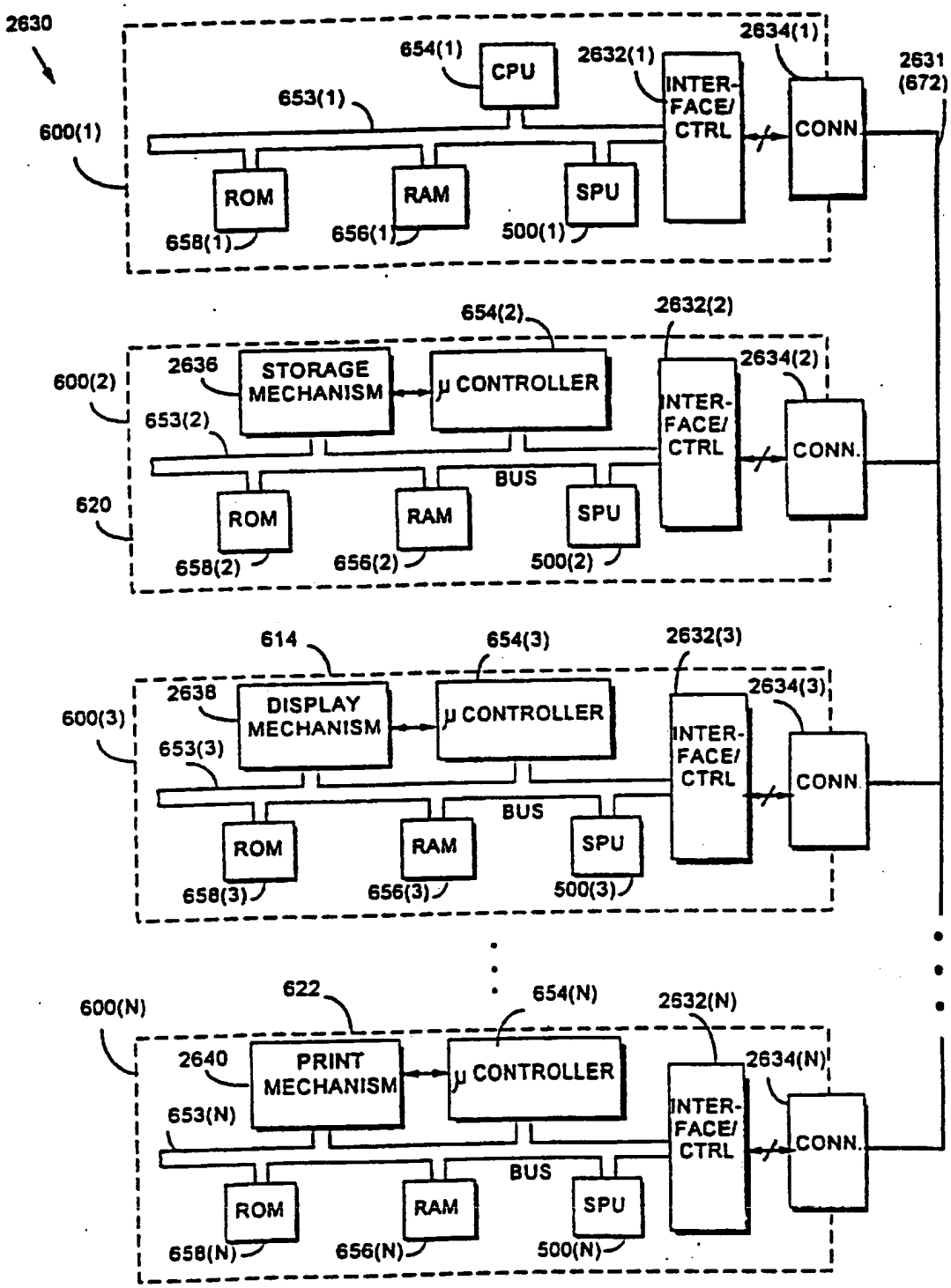
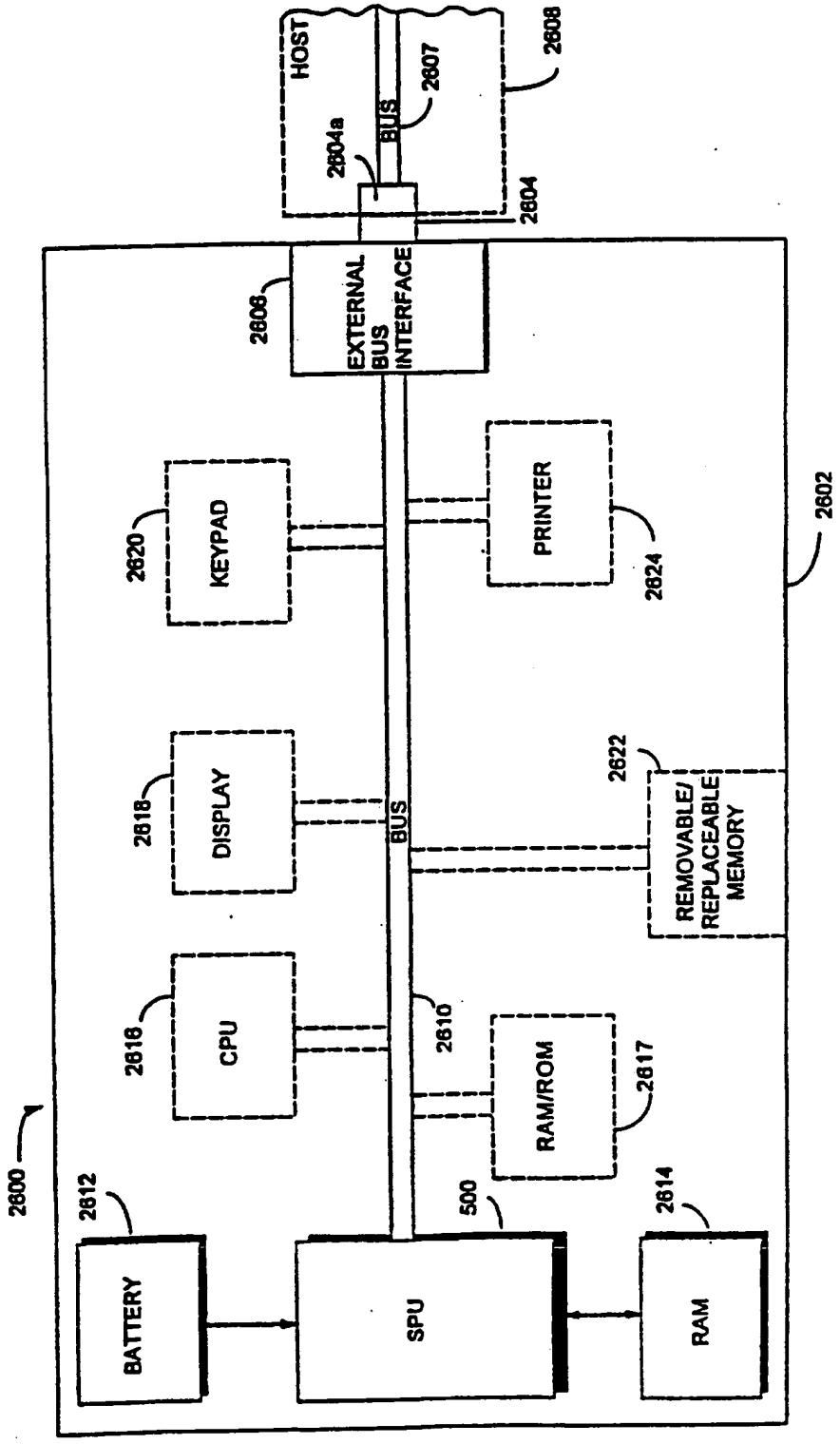

2630
600(1)
654(1)
CPU
2632(1)
INTER-FACE/ CTRL
2634(1)
2631 (672)
CONN
653(1)
ROM
RAM
SPU
658(1)
656(1)
500(1)
654(2)
2632(2)
2636
STORAGE MECHANISM
μ CONTROLLER
2634(2)
600(2)
653(2)
BUS
620
CONN.
658(2)
656(2)
500(2)
614
654(3)
2632(3)
2638
DISPLAY MECHANISM
2634(3)
600(3)
653(3)
658(3)
656(3)
500(3)
622
654(N)
2632(N)
600(N)
2640
PRINT MECHANISM
2634(N)
653(N)
658(N)
656(N)
500(N)

FIG. 70

FIG. 71

PORTABLE APPLIANCE



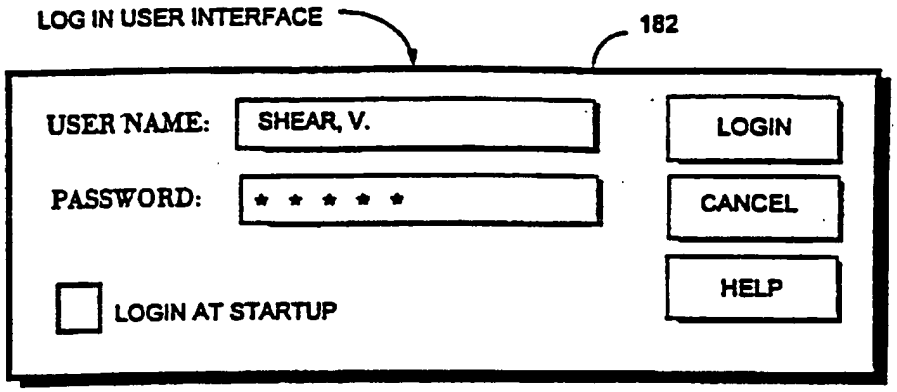


FIG. 72A

FIG. 72B

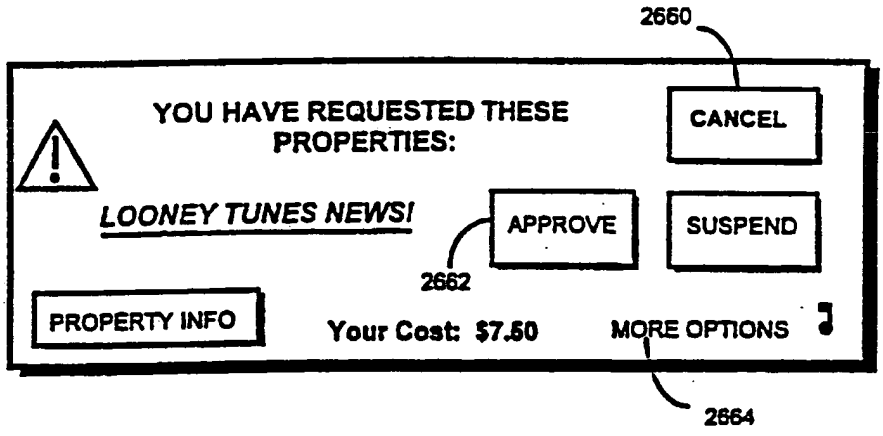


FIG. 72C

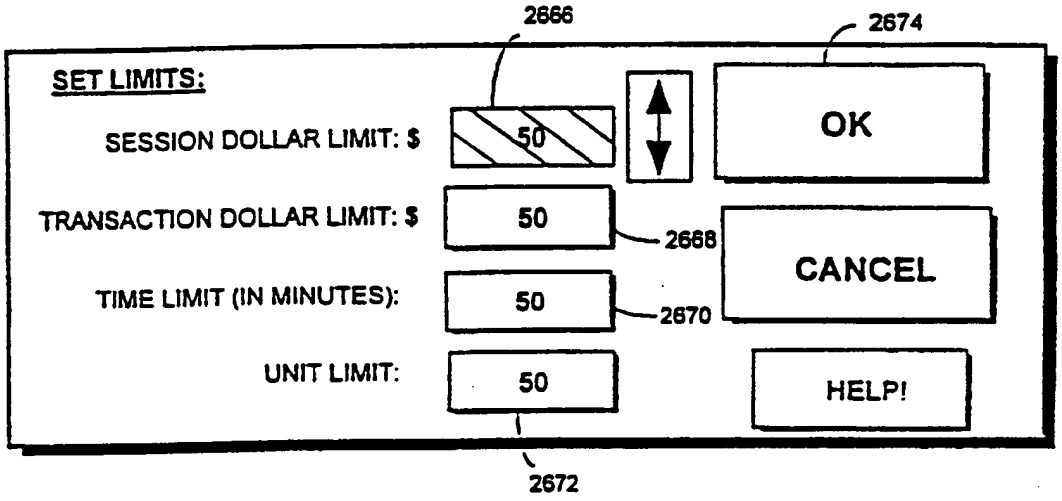

2666
2674
SET LIMITS:
SESSION DOLLAR LIMIT: $
50
OK
TRANSACTION DOLLAR LIMIT: $
50
2668
CANCEL
TIME LIMIT (IN MINUTES):
50
2670
UNIT LIMIT:
50
HELP!
2672

FIG. 72D

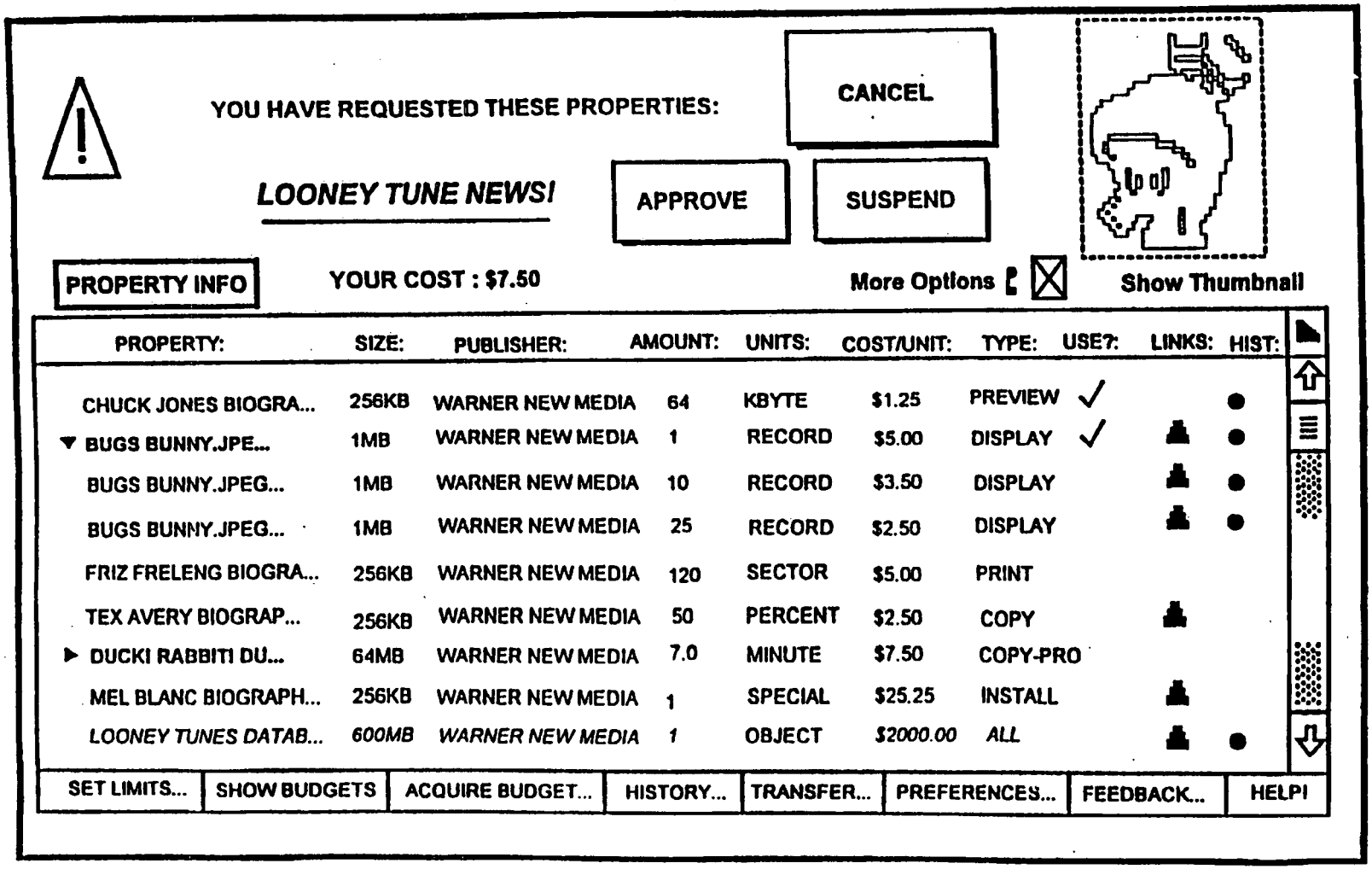

YOU HAVE REQUESTED THESE PROPERTIES:
CANCEL
LOONEY TUNE NEWS!
APPROVE
SUSPEND
PROPERTY INFO
YOUR COST : $7.50
More Options
Show Thumbnail
PROPERTY: SIZE: PUBLISHER: AMOUNT: UNITS: COST/UNIT: TYPE: USE?: LINKS: HIST:
CHUCK JONES BIOGRA... 256KB WARNER NEW MEDIA 64 KBYTE $1.25 PREVIEW
BUGS BUNNY.JPE... 1MB WARNER NEW MEDIA 1 RECORD $5.00 DISPLAY
BUGS BUNNY.JPEG... 1MB WARNER NEW MEDIA 10 RECORD $3.50 DISPLAY
BUGS BUNNY.JPEG... 1MB WARNER NEW MEDIA 25 RECORD $2.50 DISPLAY
FRIZ FRELENG BIOGRA... 256KB WARNER NEW MEDIA 120 SECTOR $5.00 PRINT
TEX AVERY BIOGRAP... 256KB WARNER NEW MEDIA 50 PERCENT $2.50 COPY
DUCKI RABBITI DU... 64MB WARNER NEW MEDIA 7.0 MINUTE $7.50 COPY-PRO
MEL BLANC BIOGRAPH... 256KB WARNER NEW MEDIA 1 SPECIAL $25.25 INSTALL
LOONEY TUNES DATAB... 600MB WARNER NEW MEDIA 1 OBJECT $2000.00 ALL
SET LIMITS... SHOW BUDGETS ACQUIRE BUDGET... HISTORY... TRANSFER... PREFERENCES... FEEDBACK... HELP!

FIG. 73

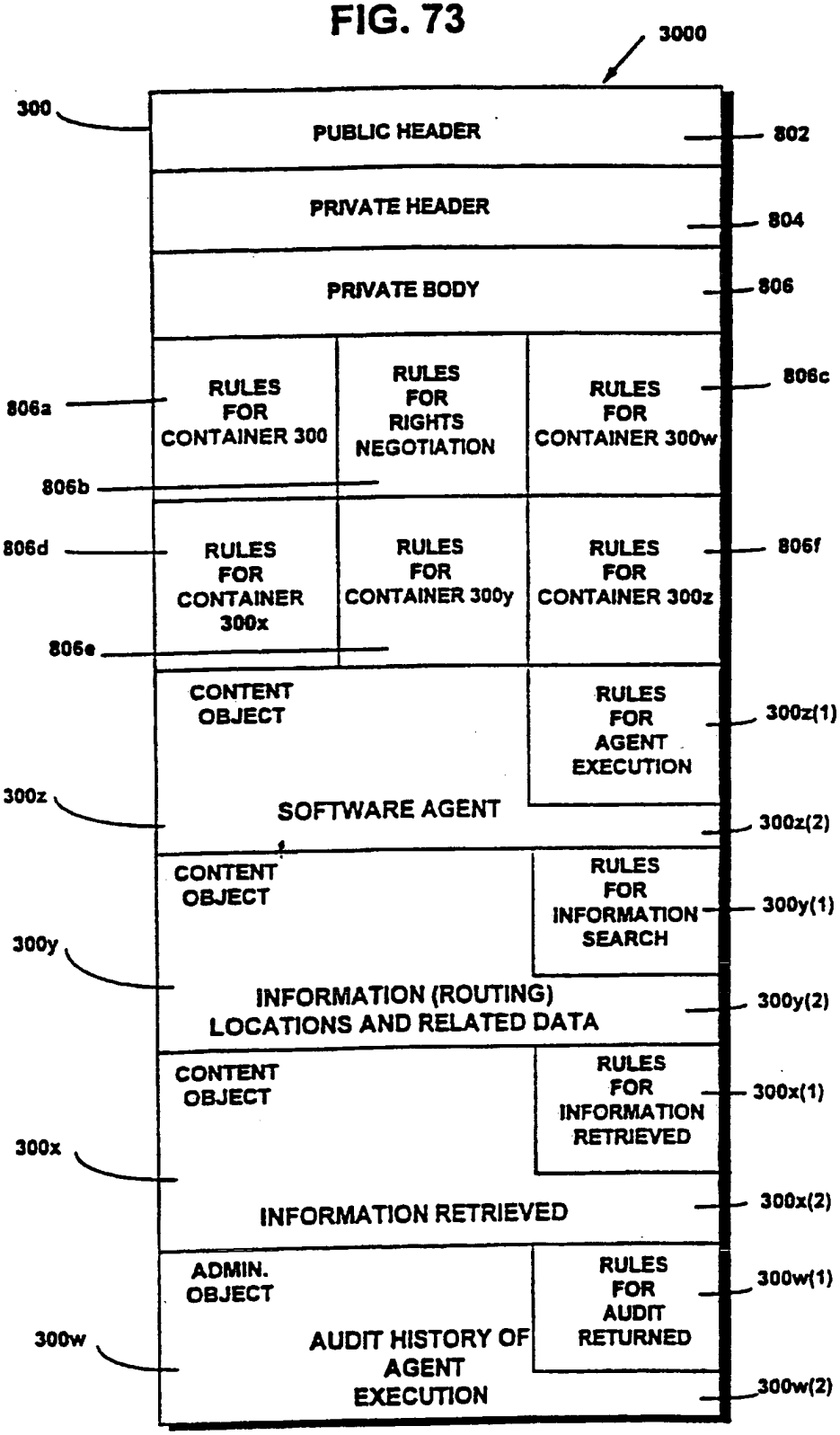

3000
300
PUBLIC HEADER
802
PRIVATE HEADER
804
PRIVATE BODY
806
806a
RULES FOR CONTAINER 300
RULES FOR RIGHTS NEGOTIATION
RULES FOR CONTAINER 300w
806c
806b
806d
RULES FOR CONTAINER 300x
RULES FOR CONTAINER 300y
RULES FOR CONTAINER 300z
806f
806e
CONTENT OBJECT
RULES FOR AGENT EXECUTION
300z(1)
300z
SOFTWARE AGENT
300z(2)
CONTENT OBJECT
RULES FOR INFORMATION SEARCH
300y(1)
300y
INFORMATION (ROUTING) LOCATIONS AND RELATED DATA
300y(2)
CONTENT OBJECT
RULES FOR INFORMATION RETRIEVED
300x(1)
300x
INFORMATION RETRIEVED
300x(2)
ADMIN. OBJECT
RULES FOR AUDIT RETURNED
300w(1)
300w
AUDIT HISTORY OF AGENT EXECUTION
300w(2)

FIG. 74

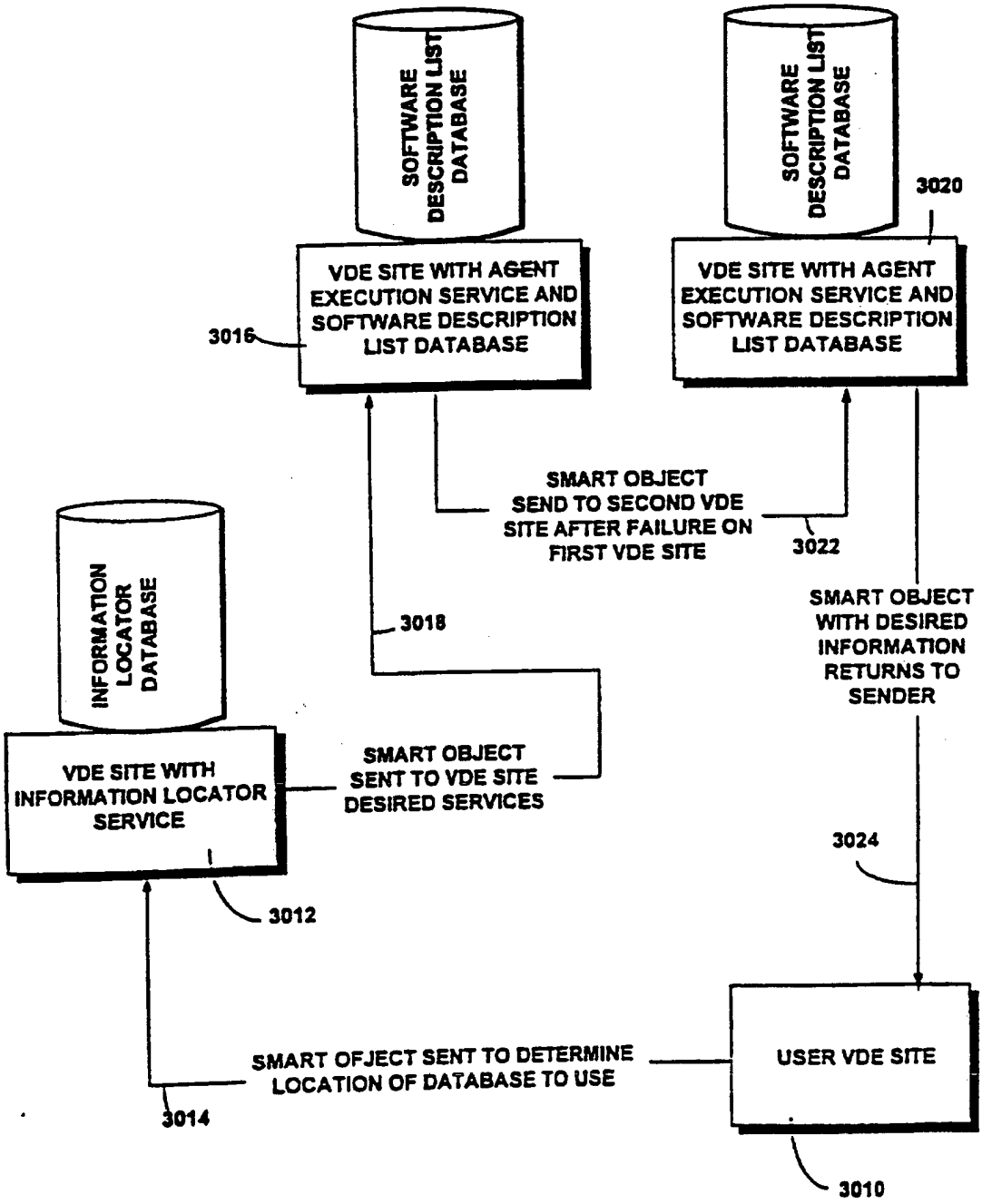

SOFTWARE DESCRIPTION LIST DATABASE
SOFTWARE DESCRIPTION LIST DATABASE
3020
VDE SITE WITH AGENT EXECUTION SERVICE AND SOFTWARE DESCRIPTION LIST DATABASE
3016
VDE SITE WITH AGENT EXECUTION SERVICE AND SOFTWARE DESCRIPTION LIST DATABASE
SMART OBJECT SEND TO SECOND VDE SITE AFTER FAILURE ON FIRST VDE SITE
3022
INFORMATION LOCATOR DATABASE
3018
SMART OBJECT WITH DESIRED INFORMATION RETURNS TO SENDER
VDE SITE WITH INFORMATION LOCATOR SERVICE
SMART OBJECT SENT TO VDE SITE DESIRED SERVICES
3024
3012
SMART OFJECT SENT TO DETERMINE LOCATION OF DATABASE TO USE
USER VDE SITE
3014
3010

FIG. 75A

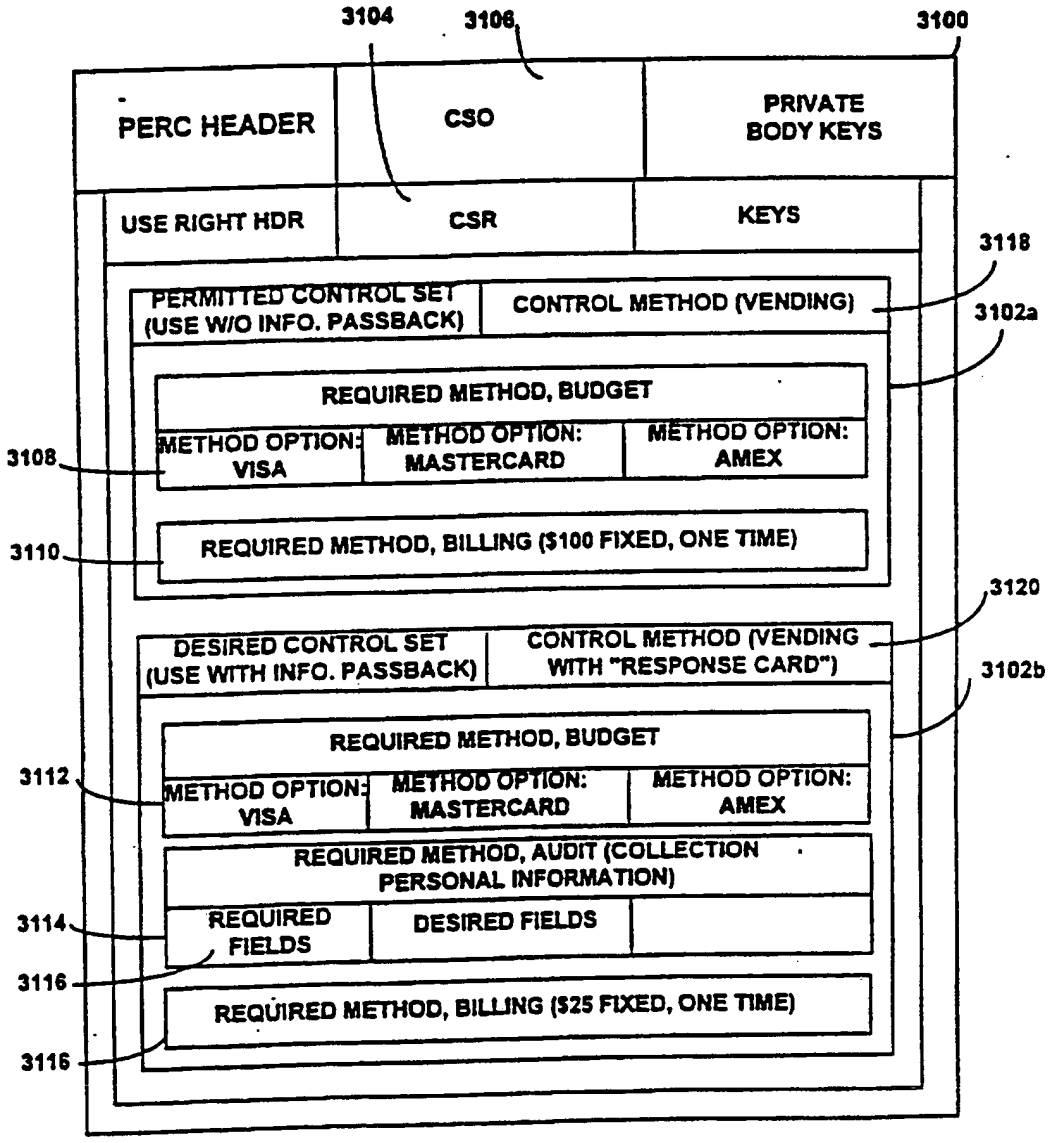

3104
3106
3100
PERC HEADER
CSO
PRIVATE BODY KEYS
USE RIGHT HDR
CSR
KEYS
3118
PERMITTED CONTROL SET (USE W/O INFO. PASSBACK)
CONTROL METHOD (VENDING)
3102a
REQUIRED METHOD, BUDGET
3108
METHOD OPTION: VISA
METHOD OPTION: MASTERCARD
METHOD OPTION: AMEX
3110
REQUIRED METHOD, BILLING ($100 FIXED, ONE TIME)
3120
DESIRED CONTROL SET (USE WITH INFO. PASSBACK)
CONTROL METHOD (VENDING WITH "RESPONSE CARD")
3102b
REQUIRED METHOD, BUDGET
3112
METHOD OPTION: VISA
METHOD OPTION: MASTERCARD
METHOD OPTION: AMEX
REQUIRED METHOD, AUDIT (COLLECTION PERSONAL INFORMATION)
3114
REQUIRED FIELDS
DESIRED FIELDS
3116
REQUIRED METHOD, BILLING ($25 FIXED, ONE TIME)
3116

FIG. 75B

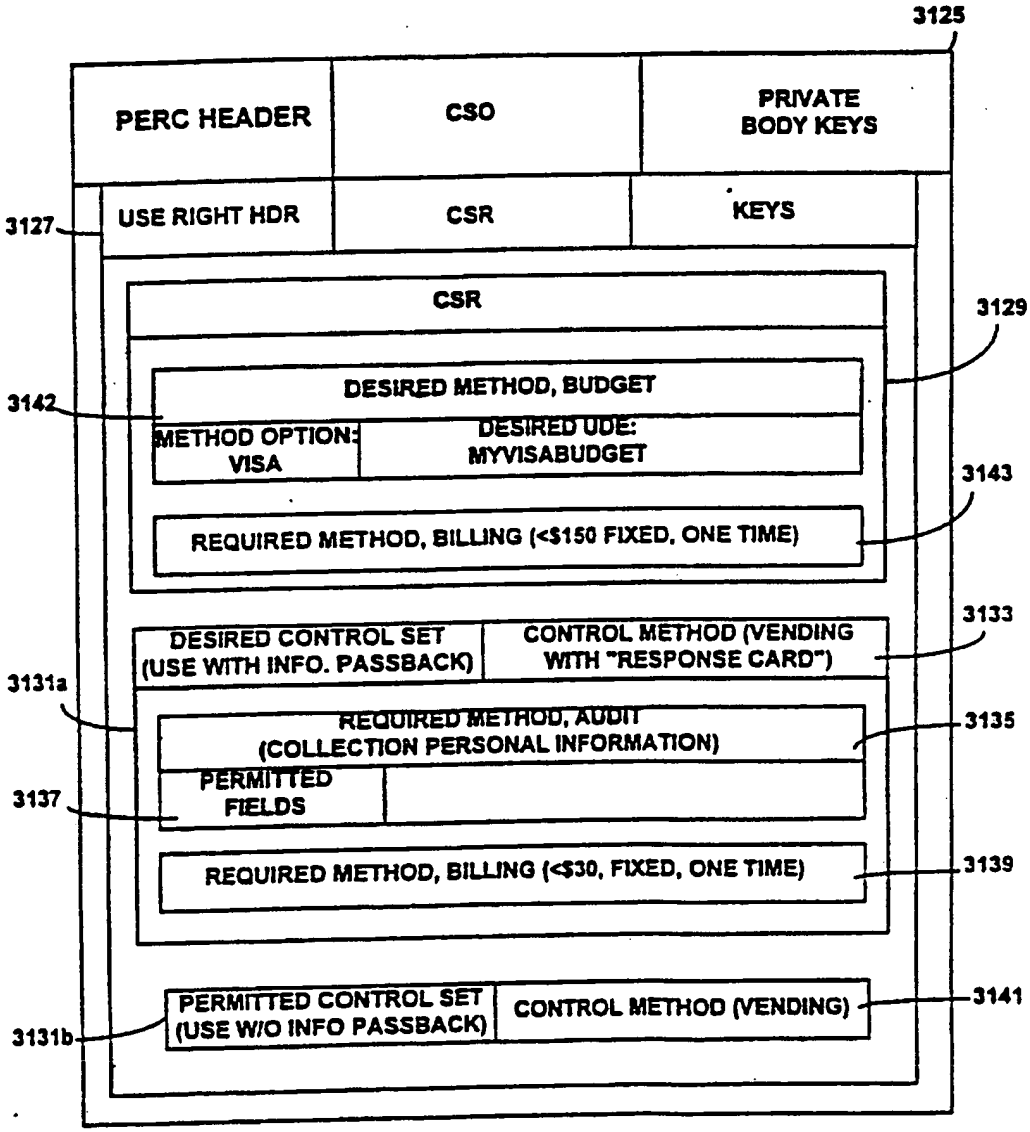

3125
PERC HEADER
CSO
PRIVATE BODY KEYS
3127
USE RIGHT HDR
CSR
KEYS
CSR
3129
DESIRED METHOD, BUDGET
3142
METHOD OPTION: VISA
DESIRED UDE: MYVISABUDGET
3143
REQUIRED METHOD, BILLING (<$150 FIXED, ONE TIME)
DESIRED CONTROL SET (USE WITH INFO. PASSBACK)
CONTROL METHOD (VENDING WITH "RESPONSE CARD")
3133
3131a
REQUIRED METHOD, AUDIT (COLLECTION PERSONAL INFORMATION)
3135
PERMITTED FIELDS
3137
REQUIRED METHOD, BILLING (<$30, FIXED, ONE TIME)
3139
PERMITTED CONTROL SET (USE W/O INFO PASSBACK)
CONTROL METHOD (VENDING)
3141
3131b

FIG. 75C

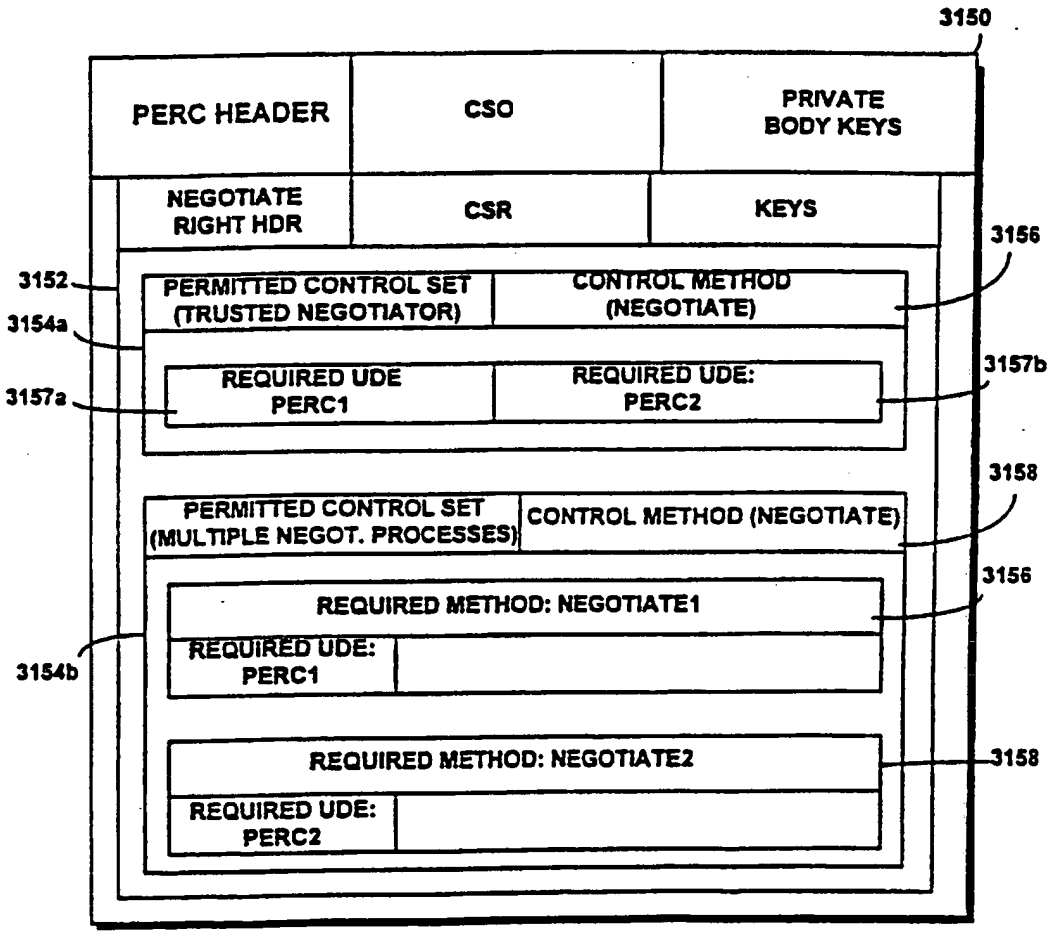
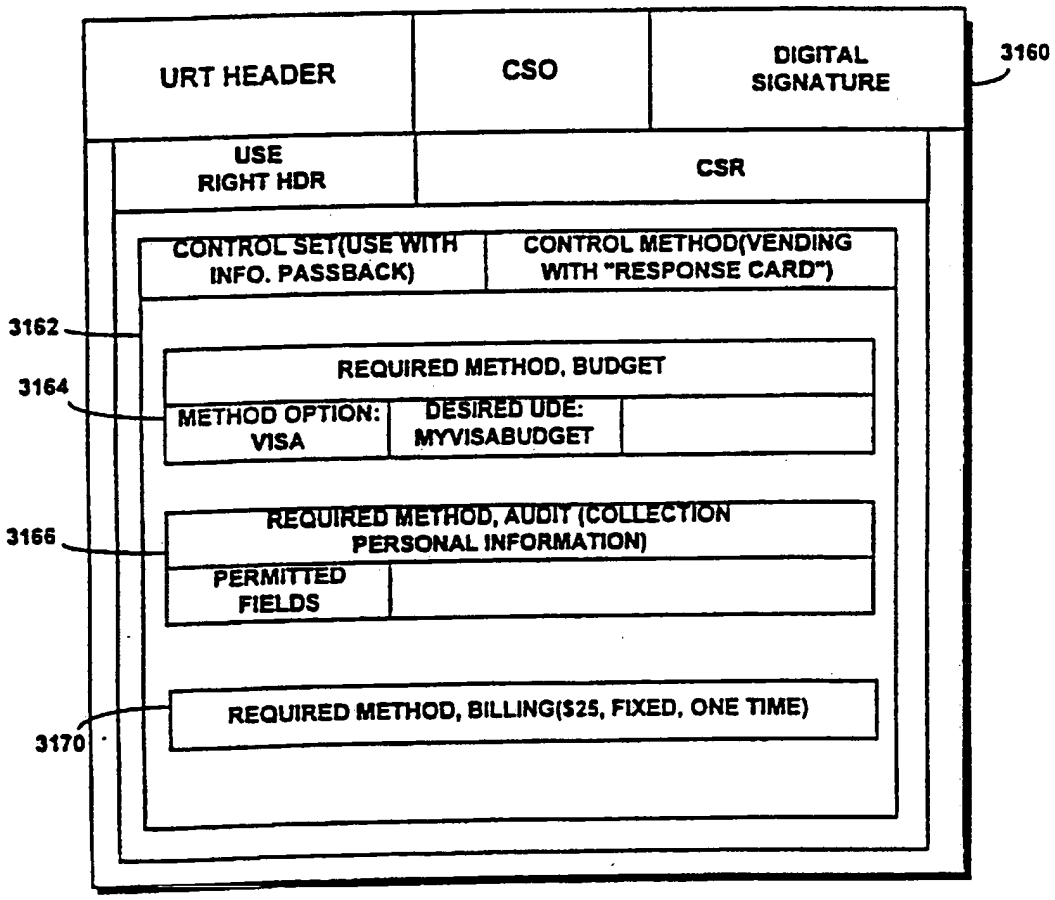

3150
PERC HEADER
CSO
PRIVATE BODY KEYS
NEGOTIATE RIGHT HDR
CSR
KEYS
3156
3152
PERMITTED CONTROL SET (TRUSTED NEGOTIATOR)
CONTROL METHOD (NEGOTIATE)
3154a
3157b
REQUIRED UDE PERC1
REQUIRED UDE: PERC2
3157a
3158
PERMITTED CONTROL SET (MULTIPLE NEGOT. PROCESSES)
CONTROL METHOD (NEGOTIATE)
3156
REQUIRED METHOD: NEGOTIATE1
REQUIRED UDE: PERC1
3154b
REQUIRED METHOD: NEGOTIATE2
3158
REQUIRED UDE: PERC2

FIG. 75D


URT HEADER
CSO
DIGITAL SIGNATURE
3160
USE RIGHT HDR
CSR
CONTROL SET(USE WITH INFO. PASSBACK)
CONTROL METHOD(VENDING WITH "RESPONSE CARD")
3162
REQUIRED METHOD, BUDGET
3164
METHOD OPTION: VISA
DESIRED UDE: MYVISABUDGET
REQUIRED METHOD, AUDIT (COLLECTION PERSONAL INFORMATION)
3166
PERMITTED FIELDS
REQUIRED METHOD, BILLING($25, FIXED, ONE TIME)
3170

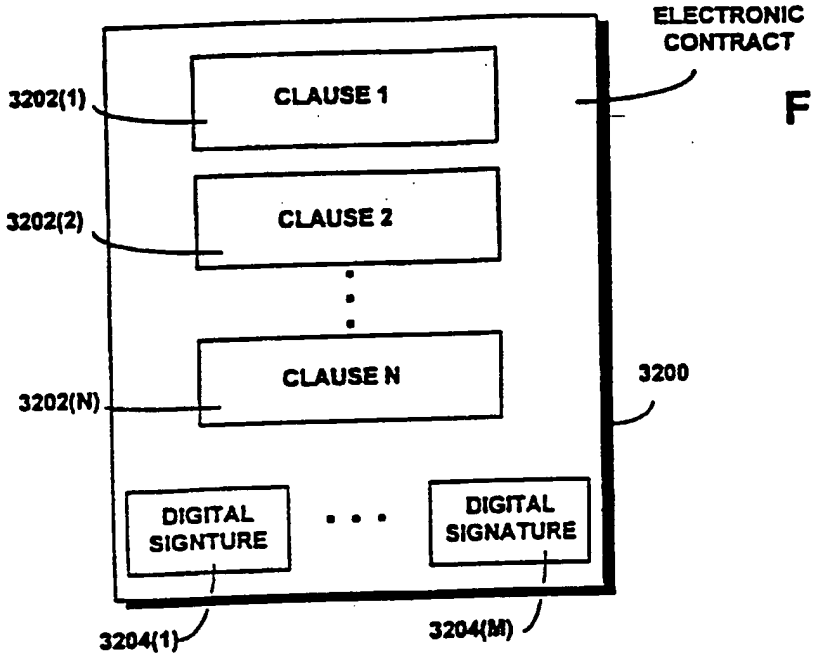


FIG. 75E

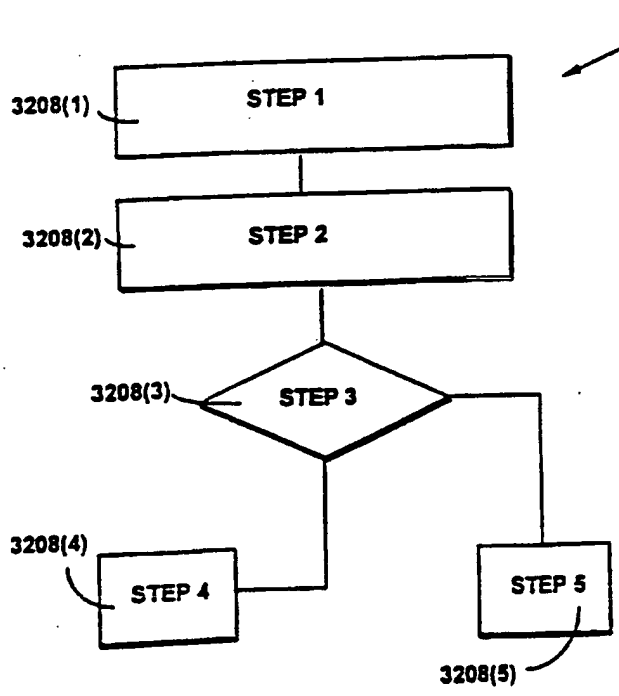


FIG. 75F

FIG. 76A

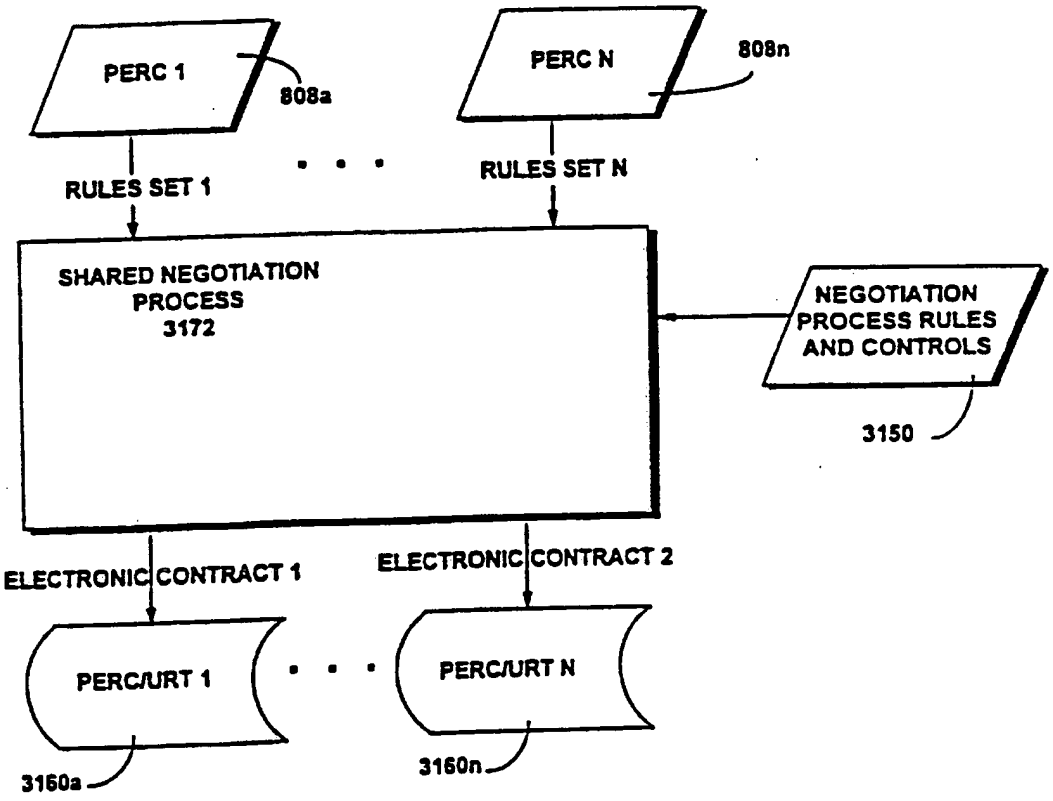

PERC 1
808a
PERC N
808n
RULES SET 1
RULES SET N
SHARED NEGOTIATION PROCESS 3172
NEGOTIATION PROCESS RULES AND CONTROLS
3150
ELECTRONIC CONTRACT 1
ELECTRONIC CONTRACT 2
PERC/URT 1
PERC/URT N
3160a
3160n

FIG. 76B

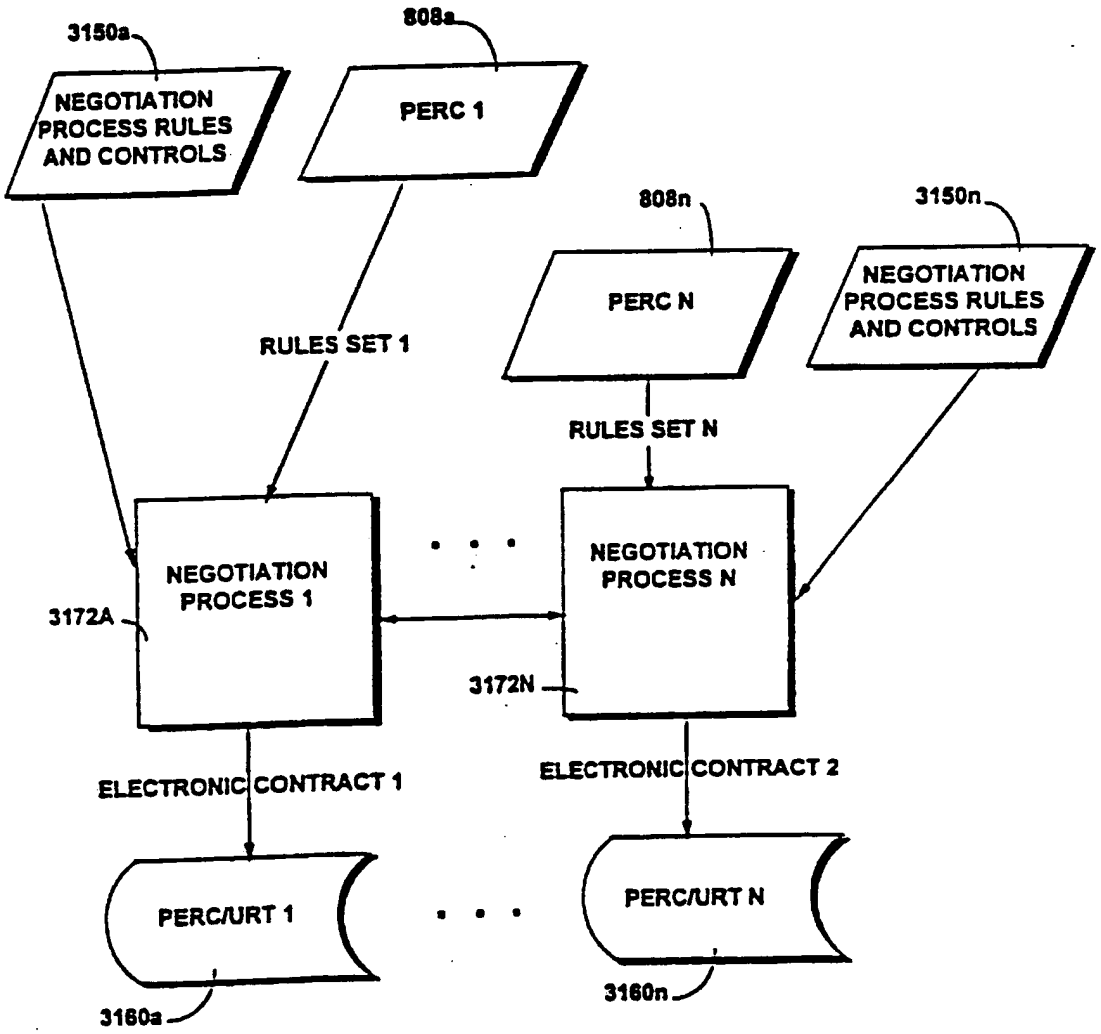
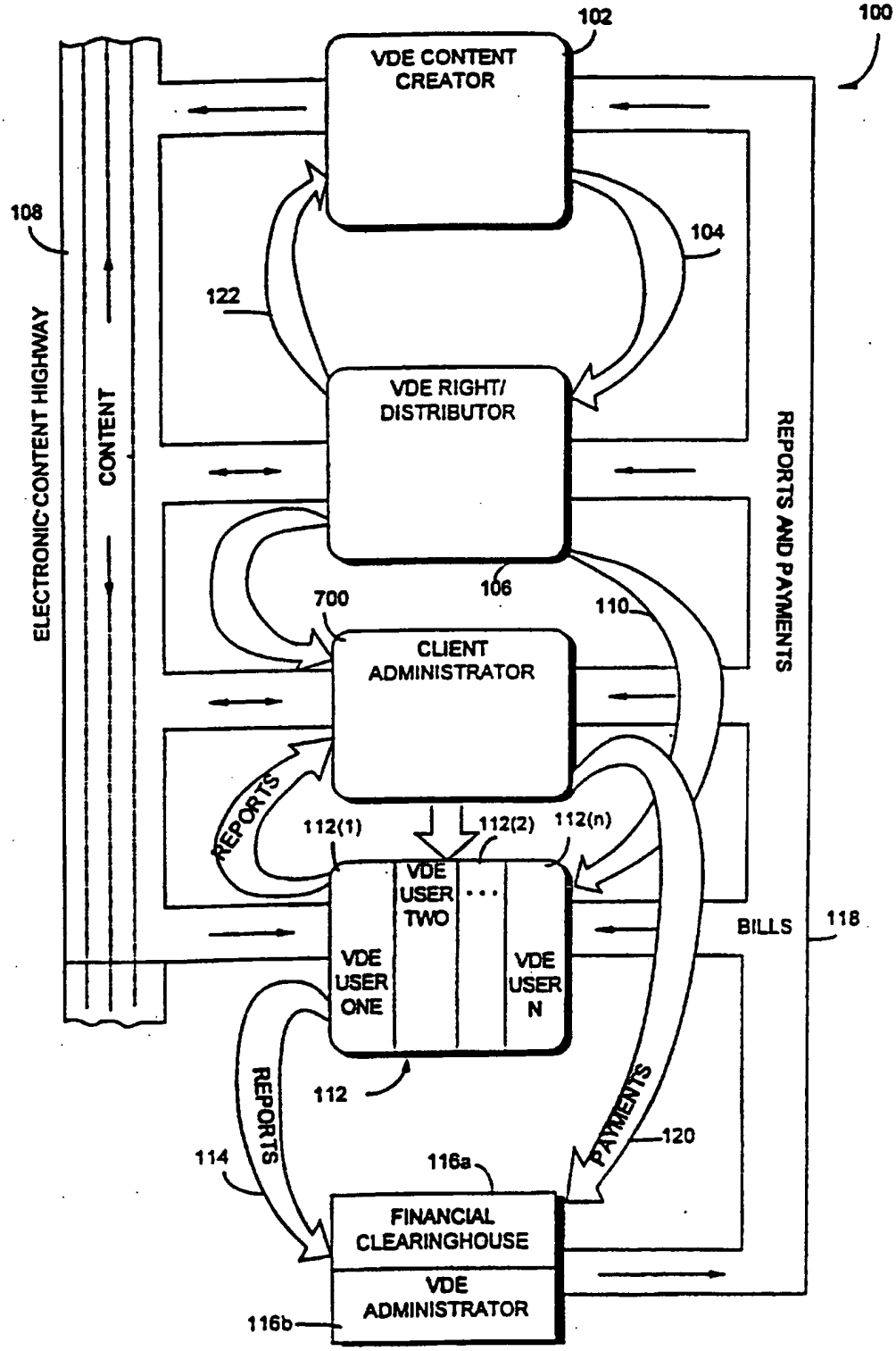

3150a
NEGOTIATION PROCESS RULES AND CONTROLS
808a
PERC 1
808n
PERC N
3150n
NEGOTIATION PROCESS RULES AND CONTROLS
RULES SET 1
RULES SET N
NEGOTIATION PROCESS 1
3172A
NEGOTIATION PROCESS N
3172N
ELECTRONIC CONTRACT 1
ELECTRONIC CONTRACT 2
PERC/URT 1
PERC/URT N
3160a
3160n

FIG. 77


102
100
VDE CONTENT CREATOR
108
104
122
VDE RIGHT/ DISTRIBUTOR
ELECTRONIC CONTENT HIGHWAY
CONTENT
REPORTS AND PAYMENTS
106
700
110
CLIENT ADMINISTRATOR
REPORTS
112(1)
112(2)
112(n)
VDE USER TWO
VDE USER ONE
VDE USER N
BILLS
118
112
REPORTS
PAYMENTS
120
114
116a
FINANCIAL CLEARINGHOUSE
VDE ADMINISTRATOR
116b

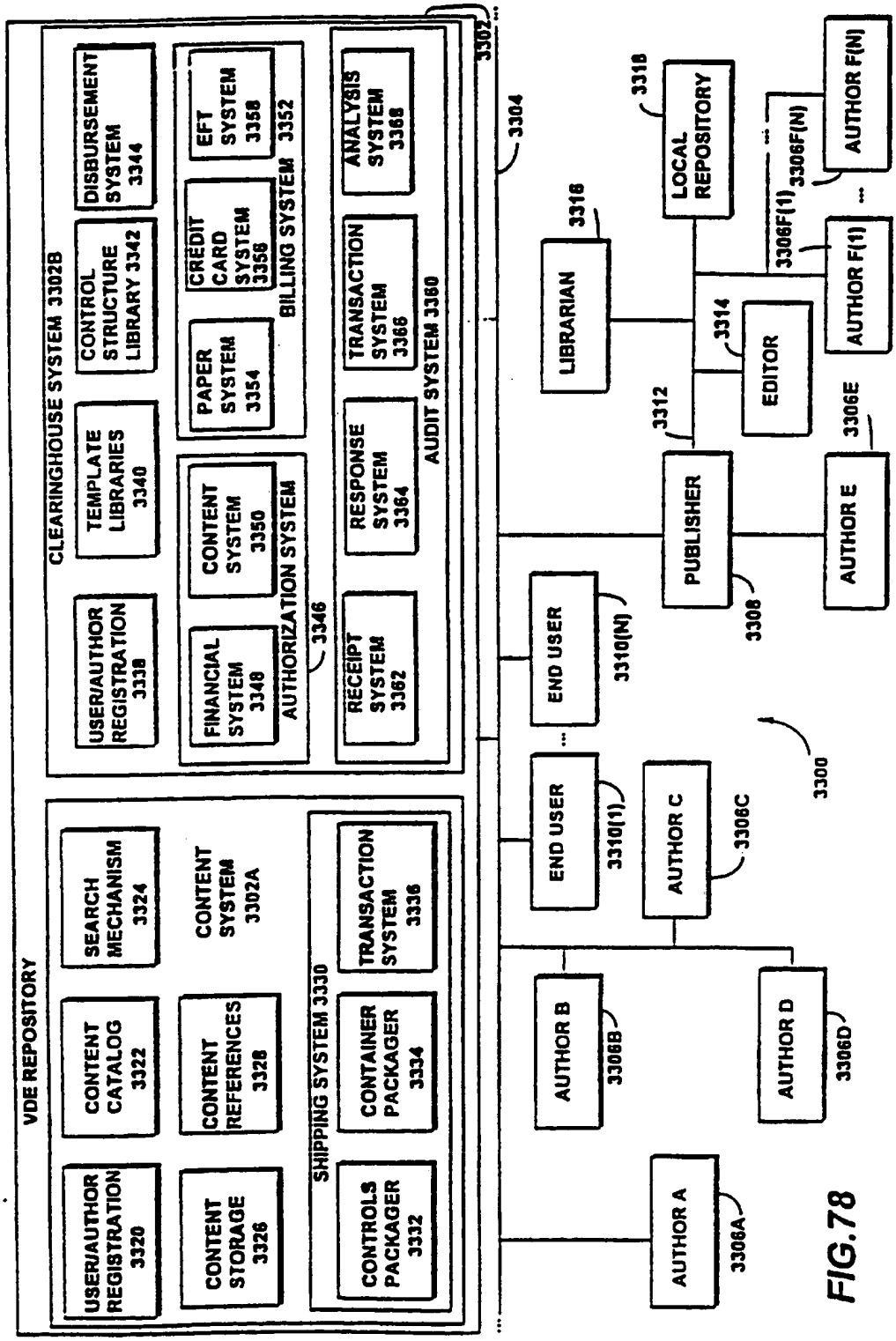

VDE REPOSITORY
USER/AUTHOR REGISTRATION 3320
CONTENT CATALOG 3322
SEARCH MECHANISM 3324
CONTENT REFERENCES 3328
CONTENT STORAGE 3326
CONTENT SYSTEM 3302A
SHIPPING SYSTEM 3330
CONTROLS PACKAGER 3332
CONTAINER PACKAGER 3334
TRANSACTION SYSTEM 3336
CLEARINGHOUSE SYSTEM 3302B
USER/AUTHOR REGISTRATION 3338
TEMPLATE LIBRARIES 3340
CONTROL STRUCTURE LIBRARY 3342
DISBURSEMENT SYSTEM 3344
FINANCIAL SYSTEM 3348
CONTENT SYSTEM 3350
AUTHORIZATION SYSTEM 3346
PAPER SYSTEM 3354
CREDIT CARD SYSTEM 3356
EFT SYSTEM 3358
BILLING SYSTEM 3352
RECEIPT SYSTEM 3362
RESPONSE SYSTEM 3364
TRANSACTION SYSTEM 3366
ANALYSIS SYSTEM 3368
AUDIT SYSTEM 3360
3302
3304
LIBRARIAN 3316
LOCAL REPOSITORY 3318
EDITOR 3314
3306F(1)
3306F(N)
AUTHOR F(1)
AUTHOR F(N)
3312
PUBLISHER 3308
AUTHOR E 3306E
END USER 3310(N)
END USER 3310(1)
AUTHOR C 3306C
3300
AUTHOR B 3306B
AUTHOR D 3306D
AUTHOR A 3306A

FIG.78

FIG. 79

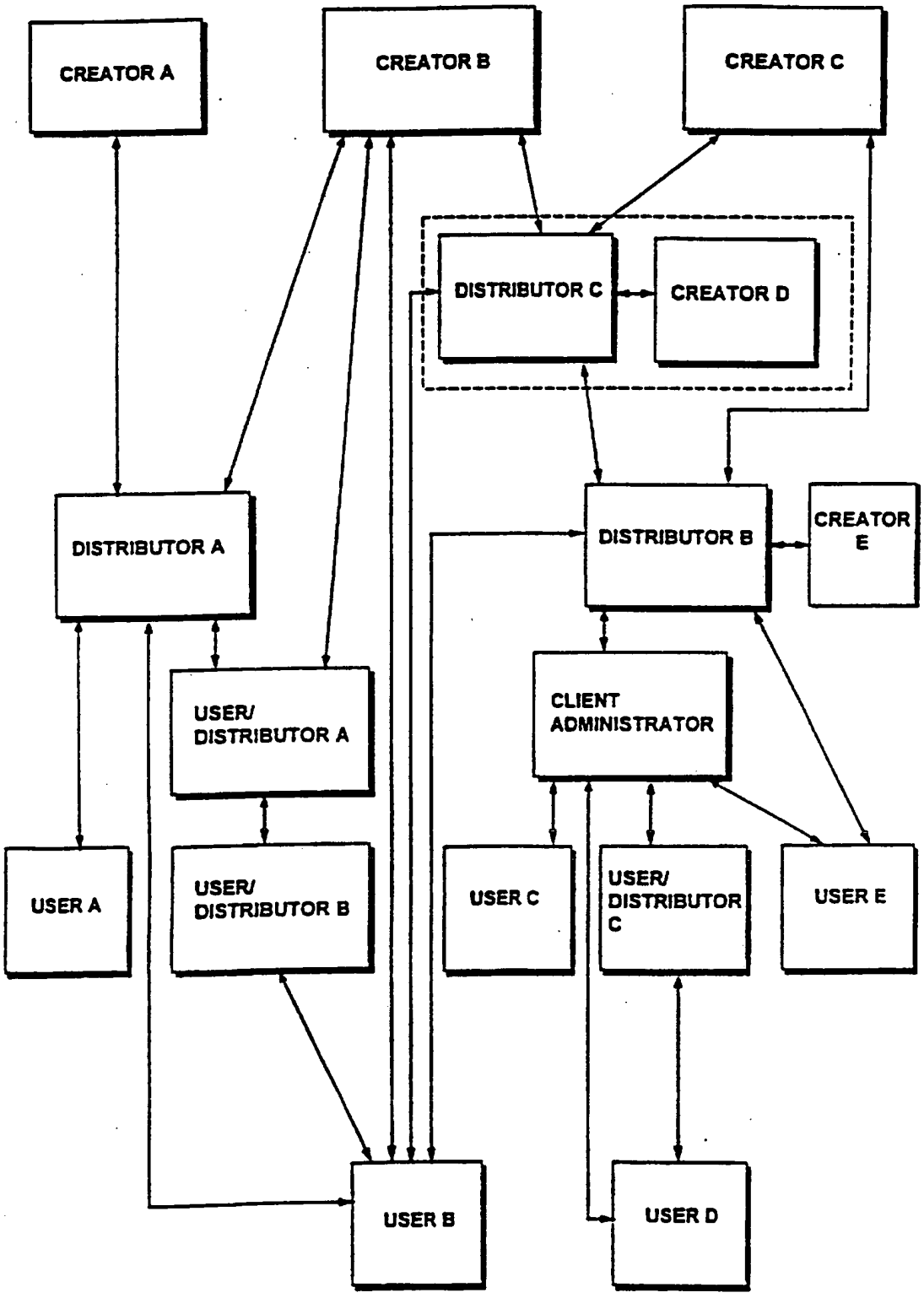
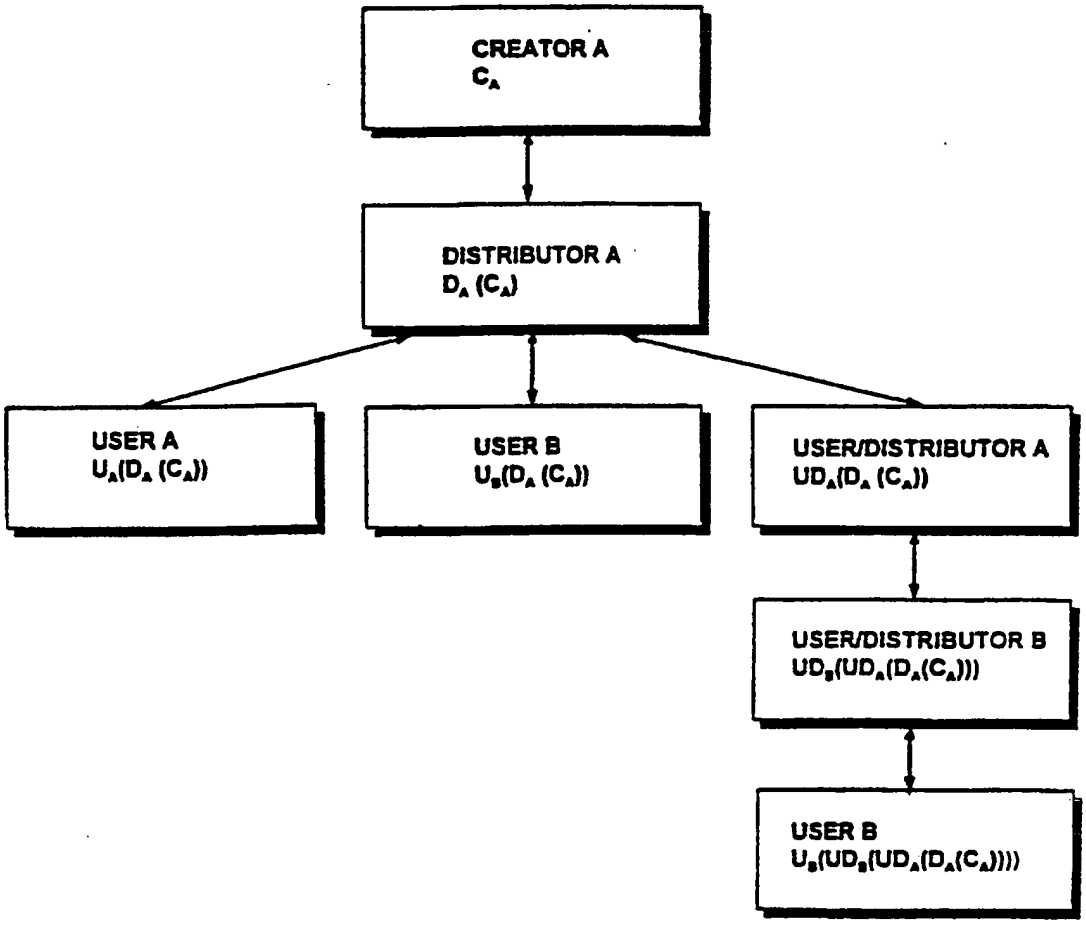

CREATOR A
CREATOR B
CREATOR C
DISTRIBUTOR C
CREATOR D
DISTRIBUTOR A
DISTRIBUTOR B
CREATOR E
USER/ DISTRIBUTOR A
CLIENT ADMINISTRATOR
USER A
USER/ DISTRIBUTOR B
USER C
USER/ DISTRIBUTOR C
USER E
USER B
USER D

FIG. 80


CREATOR A
C_A
DISTRIBUTOR A
$D_A (C_A)$
USER A
$U_A(D_A (C_A))$
USER B
$U_B(D_A (C_A))$
USER/DISTRIBUTOR A
$UD_A(D_A (C_A))$
USER/DISTRIBUTOR B
$UD_B(UD_A(D_A(C_A)))$
USER B
$U_B(UD_B(UD_A(D_A(C_A))))$

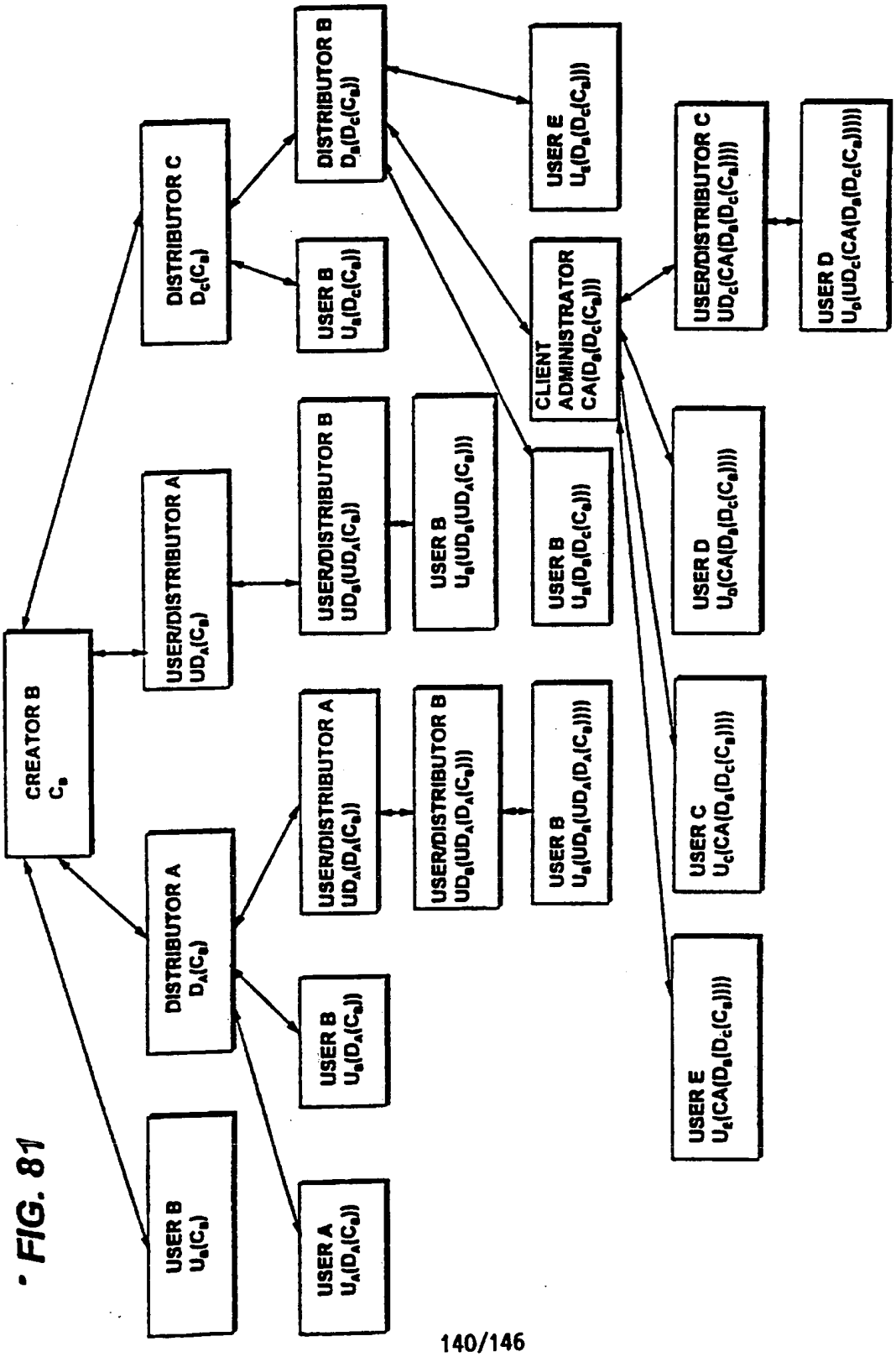

CREATOR B
C_B
DISTRIBUTOR A
$D_A(C_B)$
USER B
$U_B(D_A(C_B))$
USER A
$U_A(D_A(C_B))$
USER/DISTRIBUTOR A
$UD_A(C_B)$
USER/DISTRIBUTOR A
$UD_A(D_A(C_B))$
USER/DISTRIBUTOR B
$UD_B(UD_A(C_B))$
USER/DISTRIBUTOR B
$UD_B(UD_A(D_A(C_B)))$
USER B
$U_B(UD_B(UD_A(C_B)))$
USER B
$U_B(UD_B(UD_A(D_A(C_B))))$
DISTRIBUTOR C
$D_C(C_B)$
USER B
$U_B(D_C(C_B))$
DISTRIBUTOR B
$D_B(D_C(C_B))$
USER E
$U_E(D_B(D_C(C_B)))$
USER B
$U_B(D_B(D_C(C_B)))$
CLIENT ADMINISTRATOR
$CA(D_B(D_C(C_B)))$
USER E
$U_E(CA(D_B(D_C(C_B))))$
USER/DISTRIBUTOR C
$UD_C(CA(D_B(D_C(C_B))))$
USER D
$U_D(CA(D_B(D_C(C_B))))$
USER C
$U_C(CA(D_B(D_C(C_B))))$
USER D
$U_D(UD_C(CA(D_B(D_C(C_B)))))$

FIG. 81

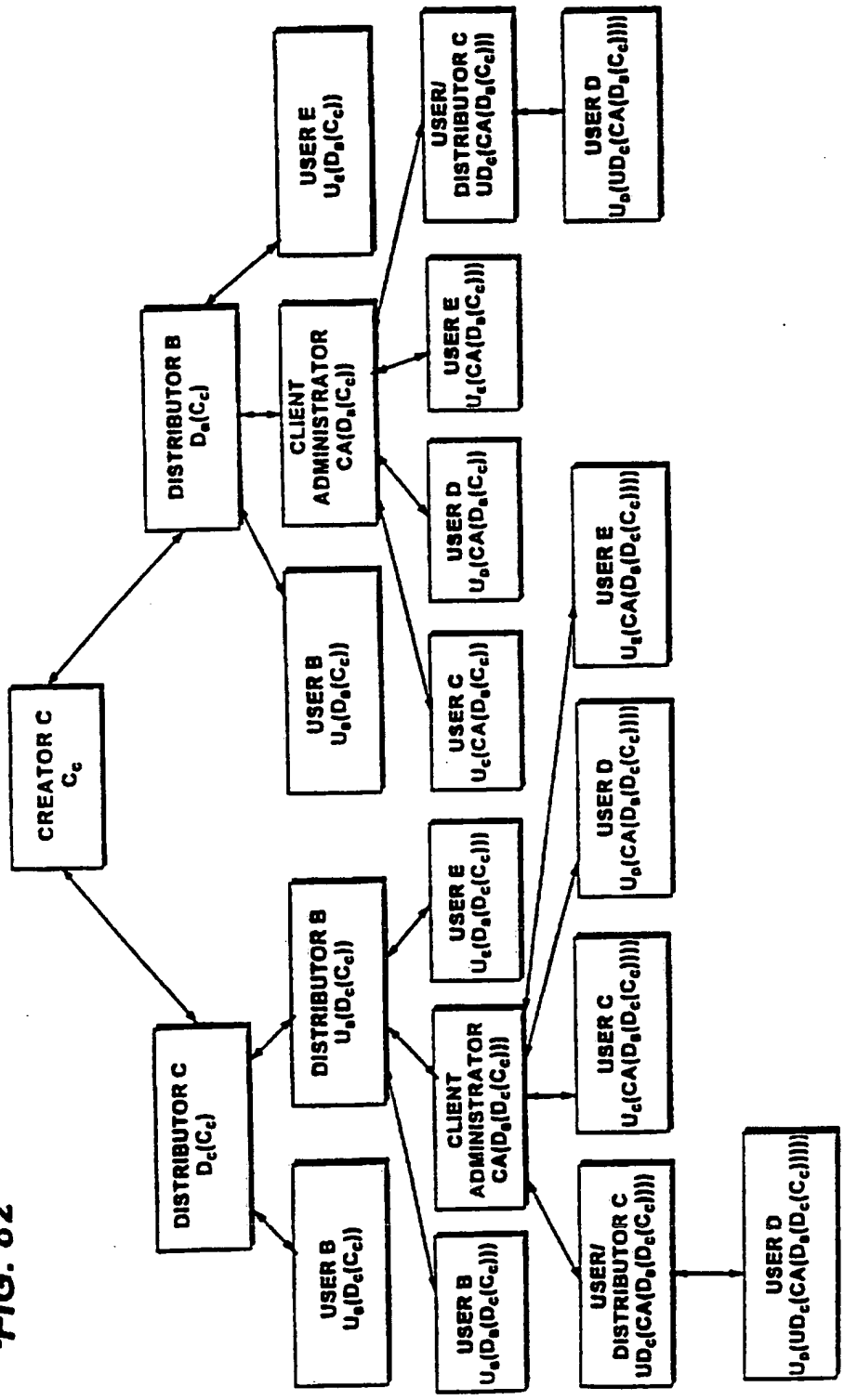

CREATOR C
C_c
DISTRIBUTOR C
$D_c(C_c)$
DISTRIBUTOR B
$D_a(C_c)$
USER B
$U_a(D_c(C_c))$
USER B
$U_a(D_a(C_c))$
DISTRIBUTOR B
$U_a(D_c(C_c))$
USER E
$U_e(D_a(C_c))$
CLIENT ADMINISTRATOR
$CA(D_a(C_c))$
USER E
$U_e(D_a(C_c))$
CLIENT ADMINISTRATOR
$CA(D_a(C_c))$
USER B
$U_a(D_a(C_c))$
USER C
$U_c(CA(D_a(C_c)))$
USER D
$U_a(CA(D_a(C_c)))$
USER E
$U_e(CA(D_a(C_c)))$
USER/ DISTRIBUTOR C
$UD_c(CA(D_a(C_c)))$
USER D
$U_a(UD_c(CA(D_a(C_c))))$
USER E
$U_e(CA(D_a(D_c(C_c))))$
USER D
$U_a(CA(D_a(D_c(C_c))))$
USER C
$U_c(CA(D_a(D_c(C_c))))$
USER/ DISTRIBUTOR C
$UD_c(CA(D_a(D_c(C_c))))$
USER D
$U_a(UD_c(CA(D_a(D_c(C_c)))))$

FIG. 82

FIG. 83

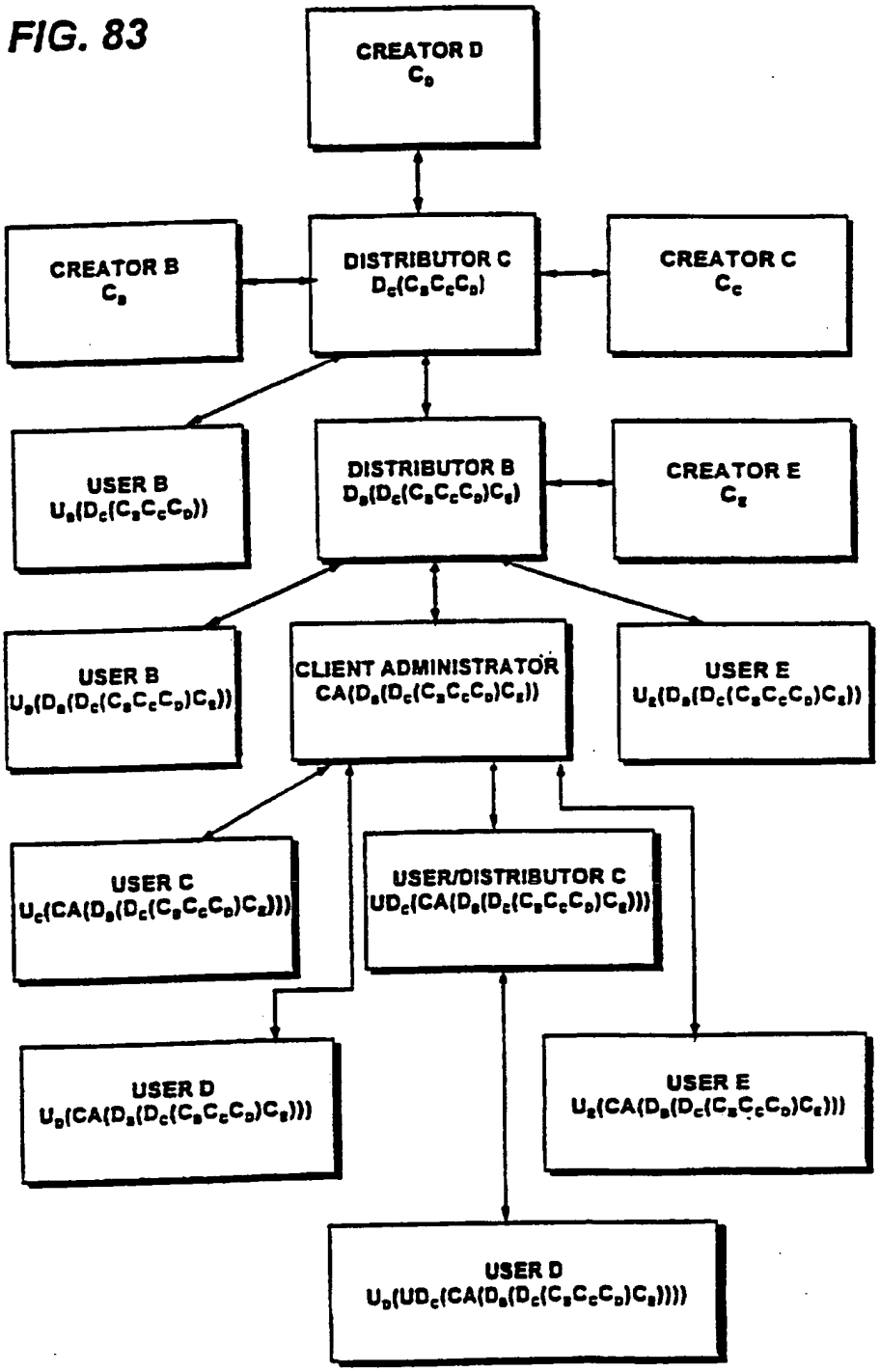

CREATOR D
C_D
CREATOR B
C_B
DISTRIBUTOR C
$D_C(C_BC_CC_D)$
CREATOR C
C_C
USER B
$U_B(D_C(C_BC_CC_D))$
DISTRIBUTOR B
$D_B(D_C(C_BC_CC_D)C_E)$
CREATOR E
C_E
USER B
$U_B(D_B(D_C(C_BC_CC_D)C_E))$
CLIENT ADMINISTRATOR
$CA(D_B(D_C(C_BC_CC_D)C_E))$
USER E
$U_E(D_B(D_C(C_BC_CC_D)C_E))$
USER C
$U_C(CA(D_B(D_C(C_BC_CC_D)C_E)))$
USER/DISTRIBUTOR C
$UD_C(CA(D_B(D_C(C_BC_CC_D)C_E)))$
USER D
$U_D(CA(D_B(D_C(C_BC_CC_D)C_E)))$
USER E
$U_E(CA(D_B(D_C(C_BC_CC_D)C_E)))$
USER D
$U_D(UD_C(CA(D_B(D_C(C_BC_CC_D)C_E))))$

FIG. 84

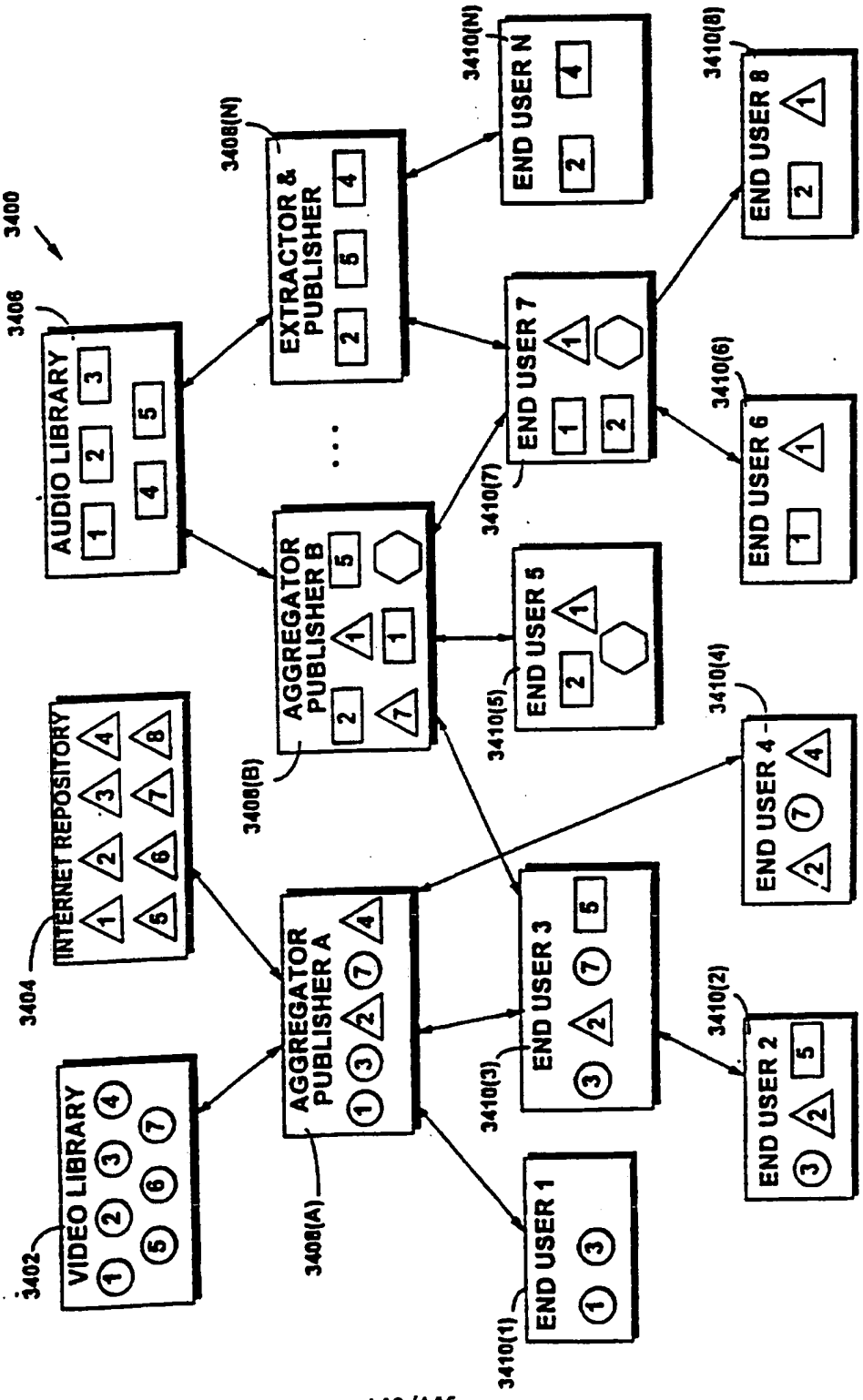
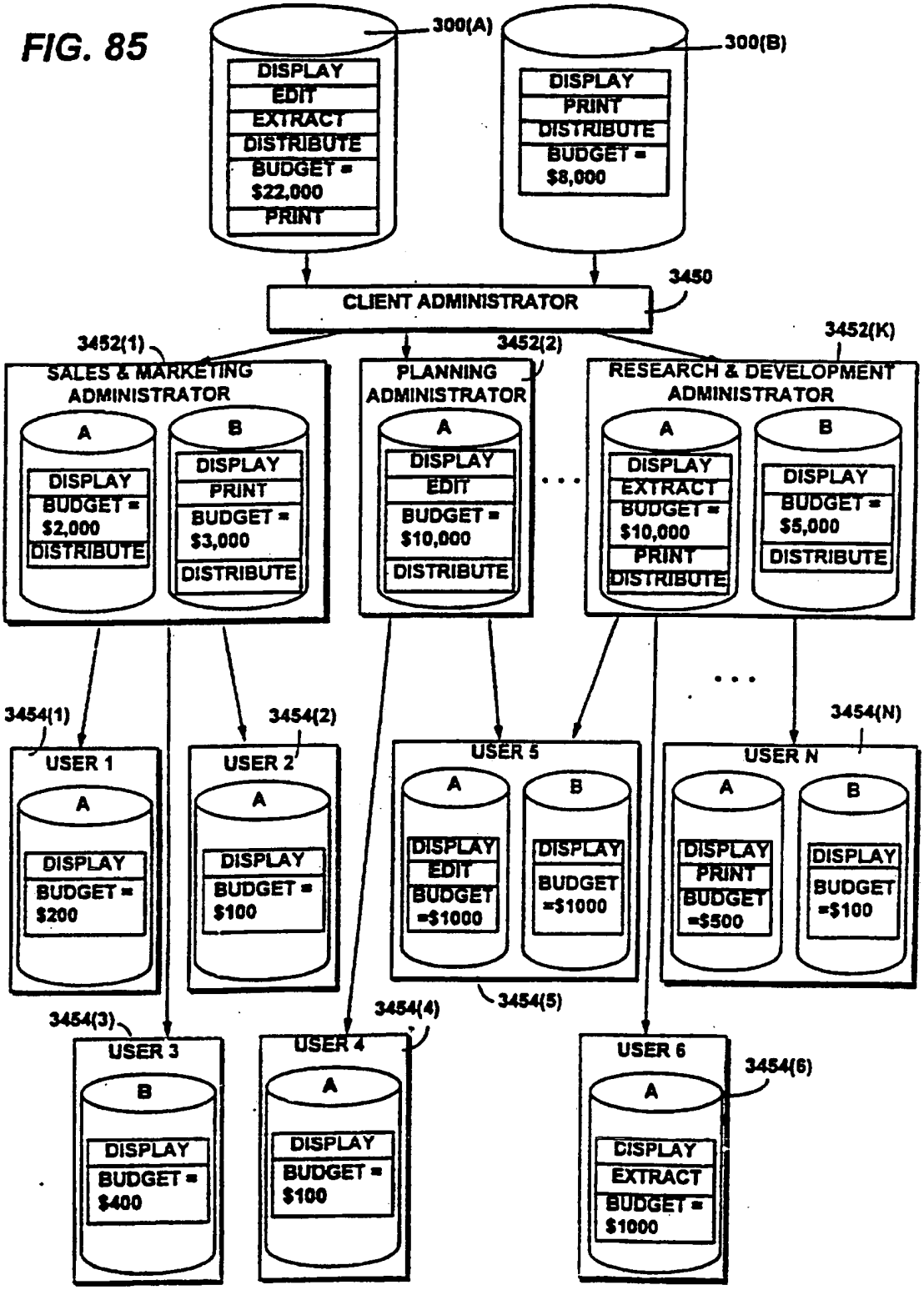

3400
3406
AUDIO LIBRARY
3408(N)
EXTRACTOR & PUBLISHER
3410(N)
END USER N
3410(8)
END USER 8
INTERNET REPOSITORY
3404
AGGREGATOR PUBLISHER B
3408(B)
END USER 7
3410(7)
3410(6)
END USER 6
END USER 5
3410(5)
3410(4)
END USER 4
VIDEO LIBRARY
3402
AGGREGATOR PUBLISHER A
3408(A)
END USER 3
3410(3)
3410(2)
END USER 2
END USER 1
3410(1)

FIG. 85


300(A)
DISPLAY
EDIT
EXTRACT
DISTRIBUTE
BUDGET = $22,000
PRINT
300(B)
DISPLAY
PRINT
DISTRIBUTE
BUDGET = $8,000
3450
CLIENT ADMINISTRATOR
3452(1)
SALES & MARKETING ADMINISTRATOR
A
DISPLAY
BUDGET = $2,000
DISTRIBUTE
B
DISPLAY
PRINT
BUDGET = $3,000
DISTRIBUTE
3452(2)
PLANNING ADMINISTRATOR
A
DISPLAY
EDIT
BUDGET = $10,000
DISTRIBUTE
3452(K)
RESEARCH & DEVELOPMENT ADMINISTRATOR
A
DISPLAY
EXTRACT
BUDGET = $10,000
PRINT
DISTRIBUTE
B
DISPLAY
BUDGET = $5,000
DISTRIBUTE
3454(1)
USER 1
A
DISPLAY
BUDGET = $200
3454(2)
USER 2
A
DISPLAY
BUDGET = $100
USER 5
A
DISPLAY
EDIT
BUDGET =$1000
B
DISPLAY
BUDGET =$1000
3454(5)
3454(N)
USER N
A
DISPLAY
PRINT
BUDGET =$500
B
DISPLAY
BUDGET =$100
3454(3)
USER 3
B
DISPLAY
BUDGET = $400
3454(4)
USER 4
A
DISPLAY
BUDGET = $100
USER 6
3454(6)
A
DISPLAY
EXTRACT
BUDGET = $1000

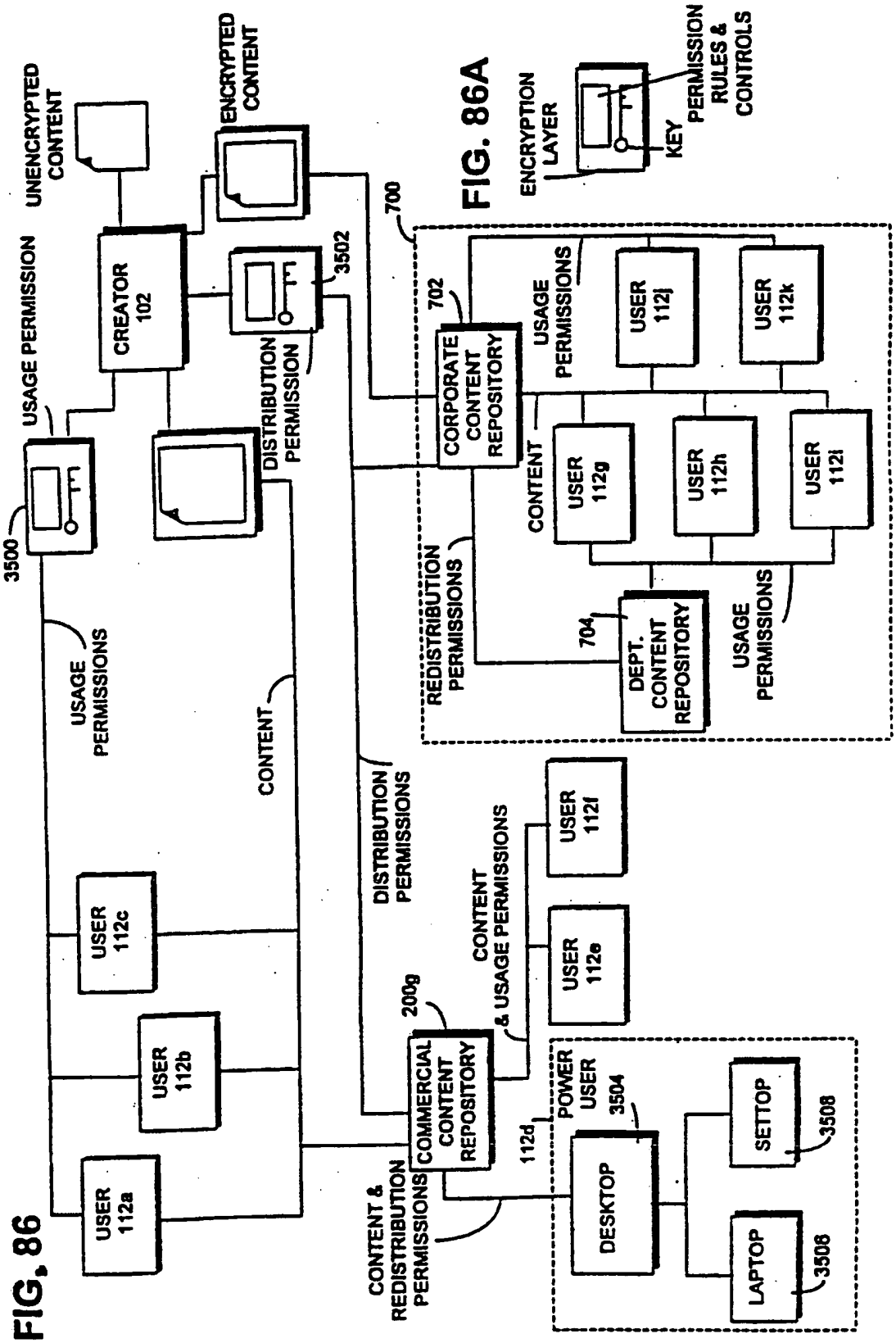


FIG. 86

FIG. 86A

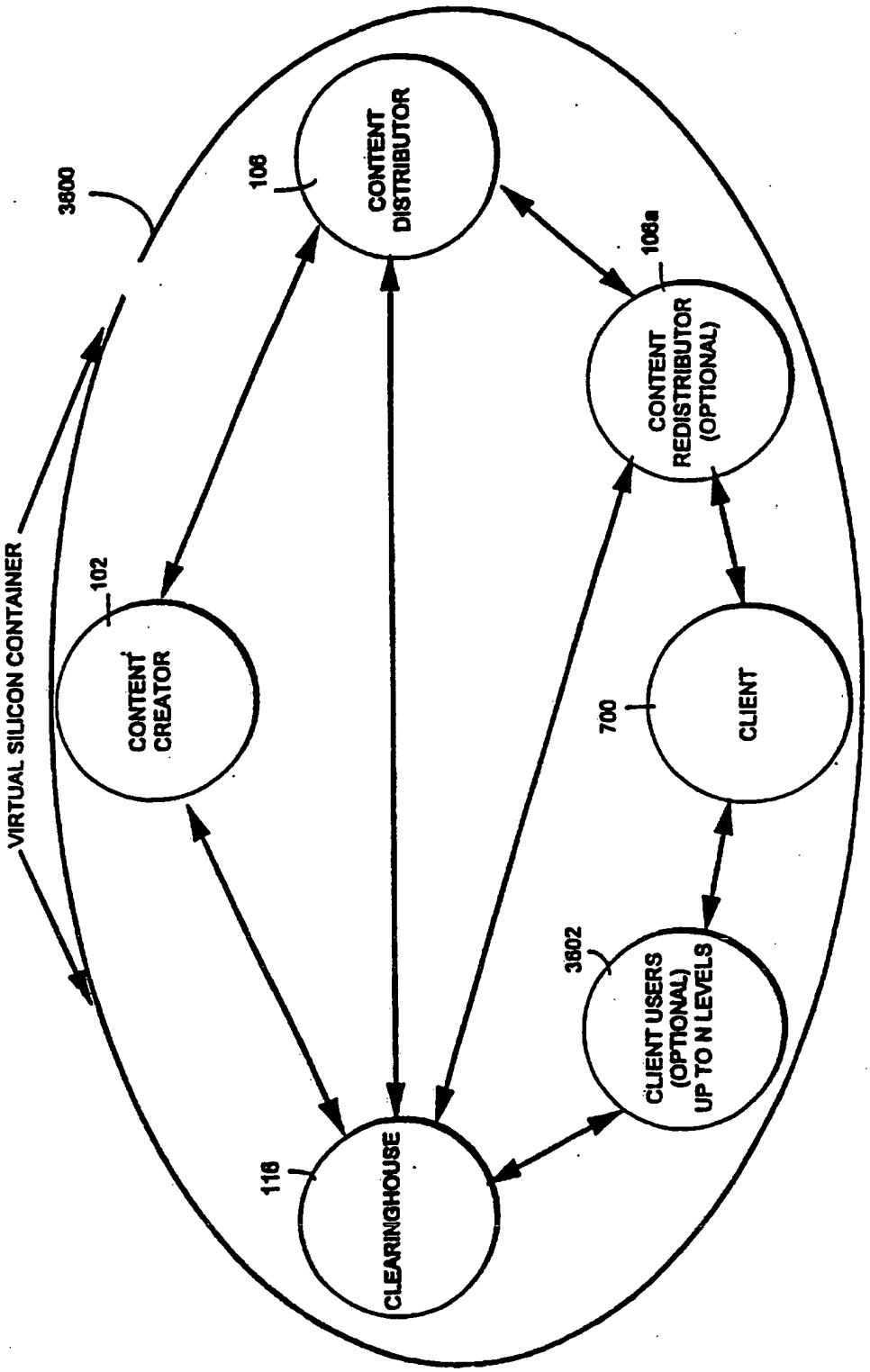

3800
VIRTUAL SILICON CONTAINER
102
CONTENT CREATOR
106
CONTENT DISTRIBUTOR
108a
CONTENT REDISTRIBUTOR (OPTIONAL)
700
CLIENT
3802
CLIENT USERS (OPTIONAL) UP TO N LEVELS
116
CLEARINGHOUSE

FIG. 87

CORRECTED VERSION*

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00, 17/60

A3

(11) International Publication Number: **WO 96/27155**

(43) International Publication Date: 6 September 1996 (06.09.96)

(21) International Application Number: PCT/US96/02303

(22) International Filing Date: 13 February 1996 (13.02.96)

(30) Priority Data:
08/388,107 13 February 1995 (13.02.95) US

(71) Applicant: ELECTRONIC PUBLISHING RESOURCES, INC. [US/US]; 5203 Battery Lane, Bethesda, MD 20814 (US).

(72) Inventors: GINTER, Karl, L.; 10404 43rd Avenue, Beltsville, MD 20705 (US). SHEAR, Victor, H.; 5203 Battery Lane, Bethesda, MD 20814 (US). SPAHN, Francis, J.; 2410 Edwards Avenue, El Cerrito, CA 94530 (US). VAN WIE, David, M.; 1250 Lakeside Drive, Sunnyvale, CA 94086 (US).

(74) Agent: FARIS, Robert, W.; Nixon & Vanderhye P.C., 1100 North Glebe Road, Arlington, VA 22201-4714 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AZ, BY, KG, KZ, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

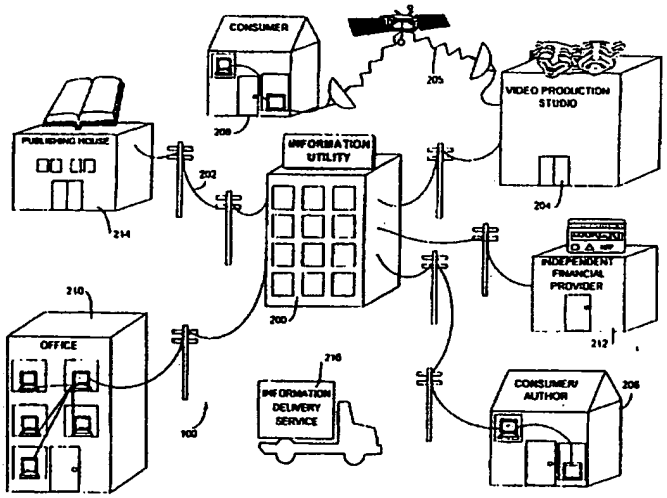
Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report: 19 June 1997 (19.06.97)

(54) Title: SYSTEMS AND METHODS FOR SECURE TRANSACTION MANAGEMENT AND ELECTRONIC RIGHTS PROTECTION



(57) Abstract

The present invention provides systems and methods for electronic commerce including secure transaction management and electronic rights protection. Electronic appliances such as computers employed in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Secure subsystems used with such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Secure distributed and other operating system environments and architectures, employing, for example, secure semiconductor processing arrangements that may establish secure, protected environments at each node. These techniques may be used to support an end-to-end electronic information distribution capability that may be used, for example, utilizing the "electronic highway".

* (Referred to in PCT Gazette No. 52/1996, Section II)

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Faso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

INTERNATIONAL SEARCH REPORT

Interna' ɳl Application No
PCT/US 96/02303

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00 G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

3

Date of the actual completion of the international search	Date of mailing of the international search report
18 April 1997	14. 05. 97
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+ 31-70) 340-3016	Authorized officer Powell, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internat ·l Application No
PCT/uS 96/02303

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 90 02382 A (INDATA CORP) 8 March 1990 see abstract; figures 2,15 see page 18, last paragraph - page 21, paragraph 2	1,2,5,6, 23,24, 62-65, 68,69, 72-77, 99-102, 133-138, 147-152, 155-158, 199,200
Y	see page 23, last paragraph - page 24, paragraph 1	21,22, 29,30, 103-108, 127-130, 223,224, 233,234, 237,238, 241-244, 504,506
A	--- -/--	61,143, 144,207, 208,245, 246, 487-500, 507-509

3

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interna al Application No
PCT/US 96/02303

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 319 705 A (HALTER BERNARD J ET AL) 7 June 1994 see abstract; figures 2,4,12	7-12, 17-20, 72-77, 133,134, 147-152, 155-158, 265-268, 298,300, 363,396
Y	see column 4, line 33 - column 6, line 24 see column 24, line 33 - column 25, line 13	21,22, 109,110, 115, 203-206, 213,214, 223,224, 237,238, 265, 302-305, 394,395
A	--- -/--	25,26, 31-38, 127-132, 207,208, 370-374, 381-384, 404

INTERNATIONAL SEARCH REPORT

Internat ! Application No
PCT/US 96/02303

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	TRANSACTIONS OF THE INSTITUTE OF ELECTRONICS, INFORMATION AND COMMUNICATION ENGINEERS OF JAPAN, vol. E73, no. 7, July 1990, TOKYO, JP, pages 1133-1146, XP000159229 R.MORI ET AL: "Superdistribution: The Concept and the Architecture"	72-77, 99-102, 127-134
Y	see abstract; figure 1 see page 1134, left-hand column, line 25 - page 1135, right-hand column, line 27	29,30, 103-108, 127-130, 233,234, 241-244, 504,506
A		31-38, 153,154, 219,220, 231,232, 370-374, 381-384, 494-497, 501-503, 511,512

X	EP 0 128 672 A (GALE IRA DENNIS) 19 December 1984 see abstract; figure 1 see page 11, line 1 - line 18	78,79, 139-142
A		80,81, 197,525

X	US 4 672 572 A (ALSBERG PETER) 9 June 1987 see abstract; figures 1,2,5,8	83,84
Y	see column 2, line 9 - column 3, line 26	109,110, 115, 302-305, 394,395
A		245,246, 253,254

Y	EP 0 565 314 A (FISCHER ADDISON M) 13 October 1993 see abstract	243,265

	-/--	

3

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 96/02303

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4 799 156 A (SHAVIT EYAL ET AL) 17 January 1989 see abstract; figure 2 see column 7, line 47 - column 8, line 54 see column 9, line 7 - column 11, line 35	42-44, 203-206, 213,214
A		153,154, 207,208, 225-228, 370-374, 381-384, 494-497, 501-503

Y	MAPPING NEW APPLICATIONS ONTO NEW TECHNOLOGIES, ZURICH, MAR. 8 - 10, 1988, no. -, 8 March 1988, PLATTNER B;GUNZBURGER P, pages 45-52, XP000215989 SIUDA K: "SECURITY SERVICES IN TELECOMMUNICATIONS NETWORKS" see the whole document	42-44
A		31-38, 55-58, 95,153, 154,231, 232

Y	EP 0 399 822 A (HEWLETT PACKARD CO) 28 November 1990 see the whole document	87-89

Y	GB 2 264 796 A (IBM) 8 September 1993 see the whole document	87-89

A	WO 92 22870 A (ICL DATA AB) 23 December 1992 see the whole document	93-98, 277-280, 306-318, 342-349, 375-379, 385, 387-393

A	US 5 343 527 A (MOORE JAMES W) 30 August 1994 see the whole document	93-98, 277-280, 306-318, 342-349, 375-379, 385, 387-393

	-/--	

3

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 96/02303

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 421 409 A (IBM) 10 April 1991 see the whole document	225-228, 245,246, 253,254
A	US 5 103 476 A (WAITE DAVID P ET AL) 7 April 1992 see the whole document	319, 321-340
A	US 5 111 390 A (KETCHAM LARRY R) 5 May 1992 see the whole document	319, 321-340
A	US 4 823 264 A (DEMING GILBERT R) 18 April 1989	
A	IBM TECHNICAL DISCLOSURE BULLETIN, vol. 37, no. 3, 1 March 1994, pages 413-417, XP000441522 "MULTIMEDIA MIXED OBJECT ENVELOPES SUPORTING A GRADUATED FEE SCHEME VIA ENCRYPTION"	
A	US 5 224 163 A (GASSER MORRIE ET AL) 29 June 1993	
A	WO 94 06103 A (HNC INC) 17 March 1994	
A	IBM TECHNICAL DISCLOSURE BULLETIN, vol. 37, no. 4B, 1 April 1994, pages 523-525, XP000451335 "TRANSFORMER RULES STRATEGY FOR SOFTWARE DISTRIBUTION MECHANISM-SUPPORT PRODUCTS"	
A	WO 94 03859 A (INT STANDARD ELECTRIC CORP) 17 February 1994	

3

INTERNATIONAL SEARCH REPORT

Ir ational application No.
PCT/US 96/02303

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see annexed sheets.

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searches without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☒ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

Inventions: 3, 6,7,9,10,24 and 29

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International Application No. PCT/US 96/ 02303

FURTHER INFORMATION CONTINUED FROM PCT/ISA/210

The following (groups of) inventions have been identified:

Invention	Claims	Subject matter
1.	1-12,17-26,29,30,61-65,68, 69,72-77,99-108,127-130, 133-138,147-152,155-158, 199,200,219-222,233,234, 243,244,265-268,294-301, 363,364,396,404,504,506	Solving problems related to: Distributing electronic information to a rightful destination using a different virtual distribution environment node (than either supplier or destination) to process the control information associated with the said digital information (cf. either of documents D1 and D2)
2.	13-16	Solving problems related to: Automating electronic processes.
3.	31-39,42-45,55-58,153,154, 203-208,213-218,223-228, 231,232,237,238,241,242, 370-374,381-384,487-489, 500,505,507-512	Solving problems related to: Electronic commerce.
4.	40,41,46-54,259-262,402	Solving problems related to: Identification of principals or principals' properties.
5.	59,60,66,67,70,71,235,236, 239,240,401	Solving problems related to: Handling electronic currency.
6.	78-81,139-144,197,525	Solving problems related to: Tamper-resistant containers.
7.	82-84,109-116,127-132, 273-276,302-305,394,395, 494-497,501-503	Solving problems related to: Audit or administrative information.
8.	85,86	Solving problems related to: Human readable interfaces.
9.	87-92,201,202,209,210,282, 283	Solving problems related to: Event or task processing.
10.	93-98,277-280,306-318, 342-349,375-379,385, 387-393	Solving problems related to: Checking component integrity or validity.
11.	117-122	Solving problems related to: Compromising a security system.

INTERNATIONAL SEARCH REPORT

International Application No. PCT/US 96/02303

FURTHER INFORMATION CONTINUED FROM PCT/ISA/210

12.	123-126	Solving problems related to: Electronic data fingerprinting.
13.	159,160,194-196,400,516, 523,524	Solving problems related to: Secure processors.
14.	161-166,517	Solving problems related to: Video controllers.
15.	167-172,175,176,518,519	Solving problems related to: Network communications.
16.	173,174,520	Solving problems related to: CD-ROM controllers.
17.	177,178,521	Solving problems related to: Set-top controllers.
18.	179-185,522	Solving problems related to: Electronic games.
19.	186-193	Solving problems related to: Multimedia communications.
20.	198,526	Solving problems related to: Detection of power supply interruption.
21.	145,146	Solving problems related to: Bitmap data structures.
22.	211,212	Solving problems related to: Modular control structures.
23.	229,230	Solving problems related to: Billing and budgeting.
24.	245,246,253,254,341, 350-353,360-362	Solving problems related to: Protected processing operations.
25.	27,28,247-252,513-515	Solving problems related to: Secure database management.
26.	263,264	Solving problems related to: Secure electronic mail.
27.	269-272	Solving problems related to: Controlling a robot.

INTERNATIONAL SEARCH REPORT

International Application No. PCT/US 96/02303

FURTHER INFORMATION CONTINUED FROM PCT/ISA/210

28.	284-293,482-486	Solving problems related to: Business automation.
29.	319,321-340	Solving problems related to: Software construction.
30.	320,369,380	Solving problems related to: Resource management.
31.	354-359,365-368	Solving problems related to: Combining or modifying data.
32.	397	Solving problems related to: Point of sale systems.
33.	398,399,490-493,498,499	Solving problems related to: Advertising.
34.	403	Solving problems related to: Renting an appliance.
35.	255-258,281,386	Solving problems related to: Rights described in software.

A concise analysis shows that the Special Technical Features of these 35 groups of claims, as determined by comparison with the features disclosed in either of documents D1 or D2, are not the same. A comparison of the objective problems related to these different groups of inventions, all seen in the light of the description and the drawings of the application, shows that these objective problems are all different and have no corresponding technical effect.

Consequently, the Special Technical Features of these different groups of inventions are neither the same nor corresponding as defined in Rule 13.2 PCT, 2nd sentence, and therefore the requirement of Unity of Invention (Rule 13.1, 2 PCT) has not been fulfilled.

Finally, it should be noted that searching the additional subject-matter of any of the groups of claims 2-35 would have involved a considerable additional search effort.

INTERNATIONAL SEARCH REPORT

...mation on patent family members

Internat... l Application No
PCT/US 96/02303

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9002382 A	08-03-90	AU 4188289 A	23-03-90
		EP 0472521 A	04-03-92
		US 5247575 A	21-09-93
US 5319705 A	07-06-94	JP 7093148 A	07-04-95
EP 0128672 A	19-12-84	WO 8404614 A	22-11-84
US 4672572 A	09-06-87	NONE	
EP 0565314 A	13-10-93	AU 3560793 A	07-10-93
		CA 2093094 A	07-10-93
		JP 6295286 A	21-10-94
		US 5390247 A	14-02-95
		US 5337360 A	09-08-94
US 4799156 A	17-01-89	CA 1281417 A	12-03-91
		EP 0370146 A	30-05-90
EP 0399822 A	28-11-90	US 5075847 A	24-12-91
		JP 3034018 A	14-02-91
GB 2264796 A	08-09-93	EP 0582681 A	16-02-94
		WO 9318454 A	16-09-93
WO 9222870 A	23-12-92	AU 660997 B	13-07-95
		AU 2022792 A	12-01-93
		DE 69203454 D	17-08-95
		EP 0588898 A	30-03-94
		ES 2078051 T	01-12-95
		FI 935541 A	10-02-94
		JP 6509430 T	20-10-94
		SE 9200604 A	13-12-92
		US 5602993 A	11-02-97
US 5343527 A	30-08-94	NONE	
EP 0421409 A	10-04-91	US 5048085 A	10-09-91
		CA 2026739 A,C	07-04-91
		JP 3237551 A	23-10-91

INTERNATIONAL SEARCH REPORT

...rmation on patent family members

Internat ...l Application No
PCT/US 96/02303

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0421409 A		US 5148481 A	15-09-92
US 5103476 A	07-04-92	CA 2095723 A	08-05-92
		EP 0556305 A	25-08-93
		JP 7089345 B	27-09-95
		JP 6501120 T	27-01-94
		WO 9209160 A	29-05-92
		US 5222134 A	22-06-93
US 5111390 A	05-05-92	NONE	
US 4823264 A	18-04-89	NONE	
US 5224163 A	29-06-93	NONE	
WO 9406103 A	17-03-94	AU 4850093 A	29-03-94
		CA 2144068 A	17-03-94
		EP 0669032 A	30-08-95
		JP 8504284 T	07-05-96
WO 9403859 A	17-02-94	EP 0606401 A	20-07-94
		JP 7502847 T	23-03-95